Role of Position of Entrepreneur in the Business on Level of Awareness of Cyber Crime

The Journal of Educational Paradigms
2023, Vol. 02(02) 181-185

ISSN (Print): 2709-202X
ISSN (Online): 2709-2038
DOI:10.47609/0301022023

Dass Munian[1], Saralah Devi Mariamdaran Chethiyar[2], Yadu K Damodaran[3]

Abstract

The cost of cybercrime is continuously increasing over the period of time. The entrepreneurial ventures play a vital role in economic growth, employment generation and total export of developed and developing countries. The detailed literature has been reviewed followed by the analysis based on the primary data collected from the entrepreneurs working in the organization. The present study is intended to evaluate the role of managers in companies and the level of cybercrime awareness. The purpose of the study was to investigate the increasing cybercrimes in Malaysia. The present study collects data using a survey questionnaire from 250 respondents using the simple random sampling technique. The current study used the PLS-SEM technique to evaluate the relationship between the level of position in organization and level of awareness of cybercrime. The findings revealed that cybercrimes are increasing because of the position of the entrepreneur in the business based on his education and experience. The study ends up with suitable recommendations.

Keywords: Position, cybercrimes, awareness, level of awareness, and entrepreneurs.

Cybercrime is recognized as a global threat which is growing rapidly along with digitalization. According to the Norton Cybercrime Report (2010), the primary objectives of the cybercriminals are to acquire information pertaining to intellectual property, business and commercial strategy, customer information including contact information, banking information, and payment card details and sensitive financial information (Bilal & Sulaiman, 2021). Additionally, Internet Organized Crime Threat Assessment (nt (IOCTA) tha) that was released in 2019 by the European Union Agency for Law Enforcement Cooperation (EUROPOL) revealed that there are six crucial domains that make up the cybercrime landscape (Chethiyar, et al., 2019). In conjunction to that, the cybercrime threat landscape in Malaysia has adopted it in the following areas which includes exploitation, cyber-dependent crime, payment fraud, cross-cutting crime factors, criminal abuse via the dark web, convergence of cybercrime and terrorism (Europol, 2019). (Allhawi et. al. 2018). has highlighted that most cybercriminals are specialists who offer different types of assistance ranging from cash-out arrangements, malware advancement, to independent exchanging items on different stages of the underground economy (Khushi, din, & Sulaiman, 2020). (Jensen, et al., 2017). also added that cybercriminals know the techniques to trick end users into opening forged emails, messages, or documents and transferring them to an Operational Technology (OT) network by using a false identity as impersonation is simple to be performed online (Hammami , et al., 2021; Qalati, et al., 2022). As a result, they target potential victims by creating mock-ups of trusted websites (such as technology and product brands) and taking advantage of the capability of obscurity in the virtual space (Abbasi, et al., 2010). Moreover, according to the Source Credibility Theory, end-users who believed or fell into the trap of the impersonated person or organization allows cybercriminals to have a lot of credibility (Boss et al., 2015). In addition to the information gathered from Interpol (2020), it was revealed that cybercriminals carry out ransomware attacks, social engineering attacks (such as phishing emails), a), and malware distributions (Riphah, et al., 2021).

In accordance with our State of Ransomware 2022 report, ransomware has affected 79% of Malaysian organizations, and 48% of those organizations claim that the number of intrusions has increased. Other reports also revealed that Malaysian business organizations have experienced a 250% increase in "ransomware" attacks in recent years. There are numerous underlying causes, including human error, configuration errors, and zero-day vulnerabilities. Cybercrime is an internet criminal activity that includes theft of information, disturbing an individual's emotions and hacking bank accounts online (Kara, & Aydos, 2022).

Around 1 million individuals fall victim to cybercrime every day, according to the Digital Crimes Unit of Microsoft Asia (January, 2019). This statistic is based on an estimate of 720 people worldwide becoming victims every minute. 10,742 incidents of cybercrime with a loss of close to RM500 million were handled by the Royal Malaysian Police in 2018.

In 2019, about 1001.51 million malware samples gathered globally were evaluated and categorized, according to statistics from the Independent IT Security Institute (AVTEST, T.I.S., 2020). Compared to 856 million in 2018, there was a 17% rise in the number of new malware detections. The European Union Agency

[1] Master's Student of Science (Correctional Science), Psychology & Counselling Program, School of Applied Psychology, Social Work and Policy, College of Arts and Sciences, Universiti Utara, Malaysia, Malaysia author: dassmunian@gmail.com
[2] University Lecturer Psychology & Counselling Program, School of Applied Psychology, Social Work and Policy, College of Arts and Sciences, Universiti Utara Malaysia, Malaysia 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. Author: yadudk023@gmail.com

for Network and Information Security (ENISA) claimed in Threat Landscape report 2018: According to (Sfakianakis, et. al., 2019). Top Cyberthreats and Trends analysis from 2019, malware is the most prevalent cyberthreat and accounts for 30% of all reports of data breach events. The developers of the virus are now altering their strategies, techniques, and procedures in order to enhance revenues and effectiveness rates, according to their study, which indicates that the danger environment for malware has altered. Contrarily, the Verizon Data Breach Investigation Report (DBIR) (Vinet & Zhedanov, 2010). underscored the significance of the data breach. Contrasted with the impact of sophisticated malware that was exploited in a variety of methods, including social engineering through the use of phishing emails, site downloads, spyware and backdoors are used to set up and carry out sophisticated assaults.

The contribution of this research will be essential in comprehending the current hazards of "Malaysian" "Cybercrime." Understanding the factors that lead to "cyber security" issues for Malaysian small and medium-sized firms would also be significant because of this study. Based on data from Malaysia, this study will help examine the negative effects of "cybercrime" on individuals and organizations (Singh, et al., 2021).

Literature Review

Cybercrime is the threat brought on by the negligent behavior of internet and computer users who use the weaknesses of computer networks and the internet medium to commit crime (Bendle, 2019). According to (Hawkins, Yen & Chou 2000). the openness of the internet medium makes it an accessible venue for cybercrime operations. Additionally, internet anonymity obscures the motivations of cybercriminals, making it more challenging to put an end to their activities (Laudon & Traver, 2016). In essence, business transactions involving the usage of the Internet pose significant dangers or hazards to both customers and suppliers if the proper security measures are not put in place (Patel & Pathrabe, 2017).

The theory of planned behavior was the theory adopted in this investigation. Icek Ajzen established the theory of planned behavior in 1985. This theory places a focus on behavioural control, subject norms, and attitudes. An attitude is a set of beliefs concerning privacy (Ajzen, 1991). The term "norma topic" describes the perceived pressure and societal pressures used to gauge particular behaviour. An organisation’s action is determined by their objectives. Behavioral control observed behaviour may have an impact on behaviour, according to this hypothesis (Ajzen, 1991).

(Yao & Linz, 2008). examined online safety behaviour using the Theory of Planned Behavior paradigm. These include the need for psychological solitude, worry about cybercrime, confidence in one's own abilities, and previous internet use. It also looks at the four online habits of comprehending privacy regulations, cleaning the memory cache on a regular basis, avoiding revealing personal information to unaffiliated parties, and determining if an online form is safe.

Furthermore, theory of reasoned action should be addressed. Fishbein and Ajzen established the Theory of Reasoned Action in 1975. According to the Theory of Reasoned Action, a person's behaviour can be affected by perception, attitude, and social influence (Ajzen, 1985). This idea can be connected to this study because it emphasizes the importance of learning something new when utilizing a computer or the internet. Internet literacy is crucial to reducing cybercrime and motivates users to stick with their online activities. Knowing how to use the internet increases one's desire to do so (Wei & Zhang, 2008).

According to research published on 12 July 2018 titled Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World, cyber-security breaches may cause Malaysia to experience a staggering economic loss of US$12.2 billion, or RM49.15 billion. This represents more than 4% of Malaysia's $296 billion gross domestic product. This report also shows that, as a result of inadequate forensics or data breach assessments, more than half of the Malaysian organizations surveyed have either had a cyber-security issue (17%) or are unaware about it (36%).

Based on this understanding of the research issue, it might be relevant to discuss the efforts made by Malaysia's government and management to protect its citizens from dangers posed by "internet connected systems" (Azhan, 2022). This process includes actions based on "hardware, software, and important data set" from cyber threats. It may be feasible to show, in light of the current situation in this country, that the Malaysian government places a lot of importance on the "security information and personal details" of its residents (Chung, et al., 2020). By doing this, the population of the nation could change. The security measures taken by this country have the ability to improve its standing abroad given the situation of the global security system.

According to Demo (Ayele Tonkolu, 2019). social media is currently the finest means to interact and engage with people all over the world. As a result, the academic student used social media to communicate with friends and family. Yet, improper social media use is what leads to cybercrime. Despite academic students using social media at an increasing rate, Near East University has not yet published a study on the self-efficacy of cybercriminals on these platforms. This study aims to find out how successfully Near East University students utilise social media to commit cybercrime on their own.

Consenting students were given a paper-based questionnaire for the purpose of conducting this study, and the 494 replies were evaluated using SPSS. To explore the self-effectiveness of cybercrime through online entertainment, the review employed the t-test technique of information analysis to identify the variation in the means of the understudy's age, orientation, and identity. The study's findings showed that there are no age differences among the dependent variables that are statistically significant in any way. The gender and nationality components on Facebook and Twitter provided an explanation for the significant mean difference. The study found that the participants' trust in their ability to defend themselves from cybercrime on social media was around average. By considering social interaction and user attitudes, the study's conclusions will ultimately be used as information by academics, students, and researchers.

Research Methodology

The researcher chose quantitative research because the data of this study can generalize and also measure the level of awareness of cybercrime in the circle of employees in Bayan Lepas, Penang. Next, the researcher also wants to test the hypothesis null by doing quantitative research. The participants in this study are people who works for small and medium-sized businesses in Gelugor area. In this study, 250 individuals from Gelugor, Penang, made up the study sample. Sample size chart by Krejcie and Morgan: number of samples available (1970). The sample included people of different ages, genders, and races. The data has been collected using the pre developed instruments from prior studies.

Analysis

The study initially conducted all the diagnostic tests to ensure that the data is normal and suitable for regression. After ensuring the hypothesis testing was performed. The result of the regression analysis revealed the following confirmation of the hypothesis testing.

Table 1: Reliability and Validity

	CA	CR	AVE
Position in organization	0.939	0.950	0.703
Level of awareness of cyber crime	0.965	0.969	0.724

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

Table 2: Hypothesis Testing

	Coeff.	S.D	T-Value	P- Values
Position in organization -> Level of awareness of cyber crime	0.634	0.081	7.797	0.000

Conclusions

This study aims to identify the level of awareness of cybercrime among entrepreneurs in recent times. The results of this survey indicate that entrepreneurs have a modest level of knowledge about cybercrime. Out of 250 respondents, 122 had a moderate degree of awareness of cybercrime, which is strongly related to their familiarity with computers. The degree of cybercrime among entrepreneurs was not significantly different between online and offline businesses, but there was a substantial variation between different employment types, including single proprietors. As a result, organizations must verify that appropriate security monitoring tools are accessible and being used. The implication of this study towards entrepreneurs is that they can know the level of awareness of cybercrime and its importance nowadays. Next, as an entrepreneur can also take steps to further increase awareness of cybercrime and avoid getting involved with cybercrime and becoming a victim of cybercrime.

The results of this study may be utilized as a preliminary evaluation to improve government actions on bettering corporate management while also raising the degree of awareness of cybercrime. To increase the cyber security of their firm currently and safeguard each entrepreneur's personal data, it is essential that they understand business management, particularly on an online platform.

The sample of this study is only taken from SMEs and does not include entrepreneurs from MNCs and other organizations. In addition, this study does not consider entrepreneurs who did not pursue their studies after SPM and this may affect the level of cybercrime awareness. Finally, some of the information gathered from entrepreneurs may be regarded as confidential and may not be disclosed to secure the privacy of their businesses.

One of the key elements that increases the risk of cybercrime occurring among business owners is a lack of understanding of the problem. The results of this study indicate that entrepreneurs have a moderate understanding of cybercrime and have earned a bachelor's degree. The only business owners who additionally showed a reasonable level of knowledge of cybercrime had degrees ranging from a diploma to a bachelor's to a master. In terms of the degree of cybercrime knowledge, there was no discernible difference between online and offline company models. However, there were discernible differences in the degree of cybercrime knowledge among various job titles within an organization. The results of this study, however, cannot be generalized because they solely concentrate on SME companies in the Gelugor, Penang area.

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.

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.

Equatora, M. A., Chethiyar, S. D. M., Rachmayanthy, R., & Susanti, N. (2022). Motivational interviewing approach in overcoming drug addicts distrust. *Available at SSRN 4040904*.

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.

Fraenkel, J., Wallen, N., & Hyun, H. (1993). *How to Design and Evaluate Research in Education 10th ed*. McGraw-Hill Education.

Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. Logistics Information Management, 15(5/6). *https://www.ahdictionary.com/. Retrieved on 10 March 2023.*

Hammami, S. M., Ahmed, F., Johny, J., & Sulaiman, M. A. B. A. (2021). Impact of knowledge capabilities on organisational performance in the private sector in Oman: An SEM approach using path analysis. *International Journal of Knowledge Management (IJKM)*, *17*(1), 15-32.

Ibrahim, A., Mahmud, N., Isnin, N., Dillah, D. H., & Dillah, D. N. F. (2019). Cyber Warfare Impact to National Security-Malaysia Experiences. *KnE Social Sciences*, 206-224.

Ibrahim, S., Nnamani, D., & Okosun, O. (2021). Types of Cybercrime and Approaches to Detection. *IOSR Journal of Computer Engineering*, *23*, 24-26.

Idris, N. (2013). *Penyelidikan dalam pendidikan*. McGraw-Hill Education.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Internet organised crime threat assessment (IOCTA) 2019. Europol. (2019). Retrieved March 1, 2023, from *https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019.*

Interpol. (2020). COVID-19 Crime: INTERPOL Issues New Guidelines for Law *Enforcement.https://www.interpol.int/en/News-and-Events/News/2020/COVID-19-crime-INTERPOLissues-new-guidelines-for-law-enforcement.*

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1-2), 203-227.

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows-based ransomware attacks. *Expert Systems with Applications*, *190*, 116198.

Kelab Keharmonian kerajaan Malaysia (KKKM). (2022). Retrieved March 10, 2023, from *https://kkkm.my/*

Khan, A. A., Asad, M., Khan, G. U. H., Asif, M. U., & Aftab, U. (2021, December). Sequential mediation of innovativeness and competitive advantage between resources for business model innovation and SMEs performance. In *2021 International conference on decision aid sciences and application (DASA)* (pp. 724-728). IEEE.

Khushi, M., Din, S. M. U., & Sulaiman, M. A. B. A. (2020). Effects of profitability measures on free cash flow; evidence from Pakistan stock exchange. *International Journal of Scientific and Technology Research*, *9*(2), 3882-3891.

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*, *8*(8), 24.

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