Data-Centric Analysis to Combat Cybercrime in Malaysia

Swee-Wei Tan[1], Kok-Why Ng[1](✉), Shereen Khan[2], and Olivia Swee-Leng Tan[2]

[1] Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia
kwng@mmu.edu.my

[2] Faculty of Management, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia

Abstract. One of the objectives of the National Policy on Industry 4.0 is to transform Malaysia's industry capabilities in both a holistic and an accelerated manner and an integral component is the adoption of appropriate legislation against the misuse of ICTs for criminal purposes. These changes, it has become the catalyst for creating a new sophisticated cybercriminal environment using more advance and complex tools to find their target victims. The study reveals that the potential economic loss in Malaysia due to cybercrime technologies can hit a staggering US$12.2 billion with the financial sector having the worst hit. Cybercrime grows with the development of technology and these figures show that there must be something lacking either in the analysis, prosecution, or the laws. To achieve a successful prosecution in cybercrime cases, Malaysia needs comprehensive new legislation which can prosecute cybercrime effectively instead of having peace meals of legislation and regulations currently. Besides, there is also a glaring insufficiency in understanding cybercrime and a tremendous lack of qualitative and quantitative data in the empirical aspects of cybercrime including the types of incidences, the analysis process, and contemporary tool support. This is primary towards shaping the intended legislation with consideration for the technological aspects.

Keywords: Cybercrime · Cybersecurity · Cybercrime Legislations

1 Introduction

Data Analytics is the method involved with guaranteeing the right analysis, cleaning, changing, and modelling data through appropriate analysis being used. Data analysis help with finding valuable subtleties, ends in supporting direction. Today, cybercrime is the consideration for all projects since National Policy on Industry 4.0 is to change Malaysia's industry capacities in the adoption of suitable legislation against the abuse of ICTs for criminal purposes [1]. Assuming the cybercrime data are examined accurately, it could without much of a stretch finish up the result and give better decisions on fighting cybercriminals with suitable legislation. Regularly, cybercrime is mistaken for

Y. C. Adam and A. W. Abdull Manaf (Eds.): ICLD 2022, ASSEHR 707, pp. 61–73, 2022.
https://doi.org/10.2991/978-2-494069-59-6_6

the demonstration that elaborates just computers and the web. However not all cybercrime included just computers and the web, for the sample, the case for Joseph Marie Jacquard [2] and another normal model would be dumpster plunging which is a strategy used to recover data that could be utilized to do an assault on a PC organization. Their demonstration isn't restricted to scanning the junk for treasures yet, in addition, to gaining admittance and secret key composed on tacky notes [3].

The cybercrime we realize today is a digital criminal demonstration perpetrated including data technologies and organizations as an instrument utilized in different illicit ways. Models, for sample, phishing, online trick, fraud buy, and others. This had quickly digital making remarkable speed and expansiveness of effect on the economy. Cybercriminals have been making steady efforts in order to stay ahead of the law's implementation indictments. Even traditional misbehaviour, such as street pharmacists, unlawful exploitation, and other traditional lawbreakers, is evolving into cyberization through the provision of E-services that reduce the chance of being traced and apprehended.

1.1 Background Study

Utilizing data advances and its application can be direct yet protecting it from cybercrime can be troublesome. There are various difficulties and perceptions that Malaysia is as yet ailing in specialized abilities while coming to cybercrime arraignments as this is taken care of by the Malaysian police contrasting and Singapore as there are gifted legislation implementation faculty managing cybercrime cases. The Cyber Security Agency of Singapore (CSA) framed on 2015 piece of Singapore Prime Minister's Office to safeguard Singapore the internet. As per the article of an assertion by Dr. Amirudin Abdul Wahab, CEO of Cybersecurity Malaysia, he sees the quick rush towards Internet of Things IoT as a test that requires different "expert abilities, however, nobody can be a specialist in all things" [4]. Malaysia's cyber security needs new abilities of faculty. There is as of now no specific cybercrime legal counsellor in dealing with cybercrime cases in Malaysia and this is a worry because of the expansion in cybercrime [6].

It shows that the absence of having the right expert, the current legislation is fundamentally falling behind as there are no specialists are checking on the current legislation to be ahead or comparable to the cybercriminal expert. Cybercrime can be planned into the accompanying activities, for sample, hacking, phishing, extortion, and others. Cyber security Malaysia measurements show that fraud has the most elevated detailed cases in 2020 [7]. Malaysia Threat Landscape 2018 [8] shows that phishing is one of the online extortion classifications which had the most elevated rate yearly. Cases detailed in many papers and findings are cybercrime gender that happened yet restricted on the analysis of recognized guilty parties' statistics in light of the cybercrime classifications and effectively indicted cases. With this data, we can recognize what are the impediments in cyber awareness or practices which cause the development in tedious announced cases. With the measurements showing development yearly in cybercrime cases, this shows a need for online security practices and Malaysia's legislation isn't adequate to battle the ascent in cybercrime.

1.2 Problem to Solve

News from Malaysiakini [10] shows that “Complete misfortunes brought about through cybercrime expanded by 24.9 percent to RM497.7 million of every 2019 from RM398.6 million the earlier year” with the best 5 episodes announced were fraud, interruption, vindictive code, content related and cyber badgering. Cybercrime is a main pressing issue to numerous nations because of its difficulties in battling them. Even though the fact that there are numerous drives taken by the public authority on forestalling cybercrimes, there is as yet an absence of abilities and tools in containing it from developing further causing a pandemic of cybercrimes [5]. The best practice for cybercrime legislation arraignments and methods against global practices in propelling nations, for sample, Singapore and the United States guaranteeing similarity and viability ought to likewise be set apart as a source of perspective and adjust in Malaysia. Malaysia had been falling behind while coming to tools and abilities in cyber legislations and proof dealing with and this is setting out freedom for cybercriminals to infiltrate further into our market [6].

Malaysia’s lawful structure should furnish legal advisors with the legitimate rule getting proof while taking care of cybercrime cases and simultaneously it should be sufficient to safeguard residents’ freedoms. J.Muller in 2019 [9] shows an expansion in web utilization from 2017 adding up to 25.3 million to 26.3 million of every 2019 which shows a normal development of roughly 1 million in 2 years or less. The projection was made that constantly 2023, it will develop to 29.4 million. There had been an expanded-on cybercrime occurrence in the year 2017 with an announced figure of 7962 episodes and the year 2019, it develops to 10,772 on detailed occurrences. This shows a pattern those cybercriminals are developing radically throughout the long term and becoming wild. The excursion to fight this cybercrime requires a decent cyber legislation development to safeguard the country, recognize and deal with cyber criminals [11].

1.3 Objective of Study

This research focus on catching the explanation of yearly expansion in cybercrime cases particularly on cyber fraud. Study on Malaysia cyber legislations correlations with the United Kingdom, United States, and Singapore guaranteeing it isn’t falling behind. This will help in recognizing current cyber legislations and the control that can be improved and how revealed cybercrime cases can be managed better. We can use the access data in the analysis of data group on the current cyber legislation indictments and these will want to help on handling cybercrime cases today and to work on in light of recognized difficulties.

2 Literature Review

The motivation behind this writing survey was to get to the condition of arising cybercrime and investigate the road of Malaysia cybercrime data analysis and the spike consistently particularly on fraud cases as need might have arisen and challenges looked by Malaysia’s legislation arraignment. Cyber security challenges are some ways or another causing significant cybercrime peculiarity in the present society. A study on understanding cybercrime in Malaysia [12] was made to have lucidity in the cybercrime definition and order to help legislation implementation offices in answering cybercriminal exercises all the more really and effectively. There had been numerous technological manifestations throughout the most recent years, like tablets, cell phones, smartwatches, and others [13].

These technology tools are helpful sooner or later they become excessively advantageous till a person dismisses the cyber security practice needs and the risks this could carry them to turning into a cyber casualty. It had turned into a typical work on putting away private significant data on technology tools only with the end goal of accommodation without changing secret key regularly founded on a survey directed more than 400 individuals. There are many kinds of cybercrimes that individuals don't know about and a significant number of these violations anybody could without much of a stretch be a cyber casualty because of their everyday practice as a web customer. This writing study will clarify further on angles on the reasons for the spike in cybercrime particularly extortion and Malaysia's legislation difficulties in battling the present cybercriminals [14].

As per the measurements report by Malaysia Computer Emergency Response Team (MyCERT) [7], which manages all security occurrences revealed by cyber casualties, MyCERT has ordered cybercrime into 9 classifications (Intrusion Attempt, Spam, Fraud, Denial of Service, Intrusion, Vulnerabilities Report, Cyber Harassment, Malicious Codes, and Content Related). Cyber occurrences statistics for the year 2019 are shown in Fig. 2 (Malaysia Computer Emergency Response Team, 2019).

Due to the digital economy outline sent off by the Prime Minister, YAB Tan Sri Dato' Haji Mahiaddin container Haji Mohd. Yassin in 2021, [26] significant climb in cyberization would be 81% of Malaysian are presently dynamic via web-based media in 2020 and 90% of government are online at this point. Simultaneously, worries on cyber security techniques on progress towards administrative arrangements command and refreshing obsolete regulations are required guaranteeing sturdiness in battling cyber assaults in the development of cyberization in Malaysia.

Digital Forensic definition which is now and again known as digital legal science is a part of analytics science enveloping the recuperation and analysis of material found in digital gadgets, regularly concerning PC crime [19]. At the Counter Terror Asia Pacific Conference in Singapore (CTAC, 2018), it was pointed out that most instances of cyber legal difficulties would be on accessing the gadget and its data and keeping away from the charge of proof altering from the extraction interaction [20].

In most revealed cases the proof is situated in a few gadgets which cause combinations between these blended gadgets data analysis drawn-out. Throughout the long term, an ever-increasing number of data are sent across digital services with higher rates of availability which will bring cyber criminological difficulties to a higher level for legislation authorization to manage. This verification that one of the legislations challenges confronted is introducing proof to the court. Cyberlaw in Malaysia as of now is with a few disengaged legislations [21].

Computer Crimes Act 1997 (like the UK's Computer Misuse Act 1990), is more on hacking, spreading of PC infections, and unapproved access. The discipline is contingent upon kinds of offenses and going from RM25,000 to RM150,000, or detainment of 3 to 10 years, or both. Communications and Multimedia Act 1998, is to control allowing licenses to organize or cyber access suppliers like Astro, Maxis, Digi, and others. They are checked by Malaysia Communications and Multimedia Commission (MCMC) being their controller on their exercises. Discipline conveys a limit of RM50,000 or as long as one year's prison, or both, upon conviction. Penal Code, is managing phishing which is a type of fraud or cheats by pantomime, online provocation, cyberbullying, and online fraud or trick. Discipline would be prison term as long as 5 years or with fine, or with both, upon conviction. For the spreading of fear-based oppressor promulgation, discipline with as long as 30 years detainment [22].

Copyright Act 1987, this is managing electronic robbery where includes taking protected materials at work explicitly. Personal Data Security Act 2010, is to guarantees web access suppliers safeguard individual data from any misfortune or unapproved access. Failing on that would be a discipline of a most extreme fine RM500,000 or as long as 3 years in prison or both. For instance, the best 3 cybercrime extortion cases which are phishing, online trick, and fraud buy fall into panel code cyber legislation in Malaysia as such a long way there is no specific legislation that was made to address these cybercrimes likewise [3].

3 Proposed Methodology

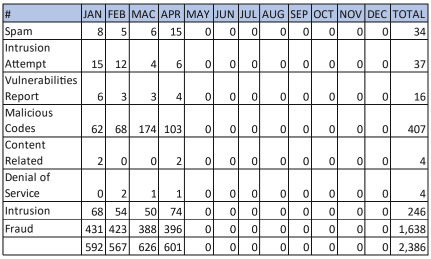
Malaysia has positioned fifth the most elevated north of 13 nations studied from Unisys that shows most worries about cyber security issues. As indicated by the yearly Unisys Security Index in 2019 of the current cyber security worries of the country [15] 88% are truly worried about bankcard extortion, 87% are truly worried about fraud and 78% are worried about hacking and infection. Cybercrime is influencing Malaysia from all perspectives paying little heed to organizations, government, or people. Statistics in Table 1 shows the sorts of cybercrime in Malaysia 2022. As per the measurements report by Malaysia Computer Emergency Response Team (MyCERT) [7], which manages all security occurrences revealed by cyber casualties, MyCERT has ordered cybercrime into 9 classifications (Intrusion Attempt, Spam, Fraud, Denial of Service, Intrusion, Vulnerabilities Report, Cyber Harassment, Malicious Codes, and Content Related). Cyber occurrences statistics for the year 2022 (Malaysia Computer Emergency Response Team, 2022).

The theoretical framework is utilized to exhibit the hypotheses and ideas that apply to this study research. This system is picked as it helps in recognizing key factors that impacted the event of the issue and concerns. This will then, at that point, move into additional assessment on factors, for sample, independent and dependent that will impact on various circumstances. Figure 1 underneath shows the schematic outline for the theoretical structure in the disclosure on battling cybercrime.

Based on the listed independent and dependent variables, the subsequent step would be identifying the proposed hypothesis. It will be illustrated as below:

H_1: There is a positive relationship between age and cybersecurity practice, cybersecurity awareness, cyber security legislation, and cybercrime statistics.
H_2: There is a positive relationship between employment and cybersecurity practice, cybersecurity awareness, cyber security legislation, and cybercrime statistics.

Table 1. Statistics on types of cybercrime in Malaysia 2022



#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	8	5	6	15	0	0	0	0	0	0	0	0	34
Intrusion Attempt	15	12	4	6	0	0	0	0	0	0	0	0	37
Vulnerabilities Report	6	3	3	4	0	0	0	0	0	0	0	0	16
Malicious Codes	62	68	174	103	0	0	0	0	0	0	0	0	407
Content Related	2	0	0	2	0	0	0	0	0	0	0	0	4
Denial of Service	0	2	1	1	0	0	0	0	0	0	0	0	4
Intrusion	68	54	50	74	0	0	0	0	0	0	0	0	246
Fraud	431	423	388	396	0	0	0	0	0	0	0	0	1,638
	592	567	626	601	0	0	0	0	0	0	0	0	2,386

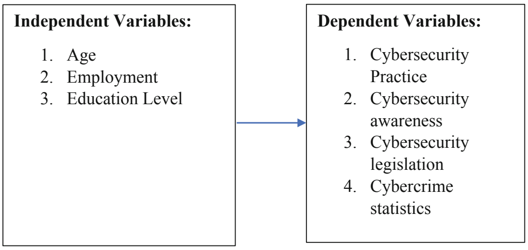


Fig. 1. Schematic diagram for the theoretical framework in the discovery on combating cybercrime

H_3: There is a positive relationship between education level and cybersecurity practice, cybersecurity awareness, cyber security legislation, and cybercrime statistics.

3.1 Data Collection

The primary data collection of this analysis is utilizing quantitative technique where the questionnaire is the fundamental tool involved a succession of questions to gather data from particular respondents. 18 Multiple decisions questionnaire is being developed for this study to ease on replying from at least 400 respondents. Respondents are given the relationship to reply at their spare energy for the given questionnaires and an aggregate of more than 400 surveys results were respondents for the analysis.

To get better data and upgrades of Malaysia cyber legislation, one more piece of this research will utilize auxiliary data collection where data was gathered as different sources, for sample, articles connected with the research subject, other's analysis on data gathered as references and diaries. It is shaped in subjective questions to gather subtleties, direction, and perceptions of 3 adjoining nations, for sample, United States, United Kingdom, and Singapore contrasting with cyber legislation in Malaysia. Before analyzing the survey data, data are prepared using excel. The data are investigated for any missing data and exceptions. The data are examined utilizing Tableau Professional Edition and Excel on measurement show tools for insightful use. Another data catching for quantitative analysis philosophy is utilizing articles, diaries, web research, and data is catch utilizing table type of correlations and to dissect.

3.2 Sampling

The objective respondents in this analysis for primary data collection would be anybody that has web access simply ready to answer the study online as study questionnaires were made utilizing google structure. The respondents take a vital part in the accomplishment of this analysis to get the required data expected for this study. The data got from this analysis was gathered from survey questionnaires convey to irregular web customers like companions, associates, understudies, and others. Respondents are accepted to answer the study surveys sincerely with no impact. The assessed number of respondents would be at the very least 400 respondents' data because of sample size assurance that will be gathered and utilized for a logical reason. These respondents additionally used to catch data for secondary data collection respect to Malaysia's legislation part.

Factors being considered on this sample size assurance:

1. Population size
   The size of Malaysia's populace in 2021.
2. Margin of error (certainty level span)
   This depends on security buffer resilience level. A room for mistakes ±5% is being utilized.
3. Confidence level
   Certainty level of 95% is being use since a wiggle room 5% is set.
4. Standard deviation
   To estimated how much the reactions to get will vary from one another and from the mean number. 5 is utilized to be protected guaranteeing sample size is sufficiently enormous.

Next would transform the certainty level into Z-score as underneath [59,60].

Z-score otherwise called standard score address how a long way from the mean a data point is. It's a proportion of the number of standard deviations underneath or over the populace mean a crude score is

Z Score = $(x - \mu)/\sigma$
x = Datapoint = 0.95
μ = Mean = 1.93
σ = Standard deviation = 0.5

$$\begin{aligned} Z\ score &= \frac{x-\mu}{\sigma} \\ &= \frac{1.93 - 0.95}{0.5} \\ &= 1.96 \end{aligned}$$

P-value from Z-Table:

$P(x < 1.93) = 0.975$
$P(x > 1.93) = 1 - P(x < 1.93) = 0.024998$

P(.95 < x < 1.93) = P(x < 1.93) − 0.5 = 0.475
90% – Z Score = 1.645
95% – Z Score = 1.96
99% – Z Score = 2.576

Necessary Sample Size = (Z-score)2 ∗ StdDev ∗ (1 − StdDev)/(margin of error)2 using 95% confidence level, .5 standard deviation, and a margin of error (confidence interval) of ±5%.

$$
\begin{aligned}
&((1.96)2 \times .5(.5))/(.05)2 \\
&= (3.8416 \times .25)/.0025 \\
&= .9604/.0025 \\
&= 384.16
\end{aligned}
$$

385 respondents are needed.

For secondary data collection, this will be making use of the available research data or data available online or offline and also details such as news, journals and other relevant data group.

4 Result

This section explains the analysis philosophy that has been utilized in this study. It sums up the methodology taken to direct the analysis, beginning with a presentation of the research technique all in all, presumptions, carefully describing the situation on the research calculation, and afterward explaining on phases of the research strategy on every one of the interactions. This comprises the analysis model, hypotheses, approach, and strategies.

Generally, the study of my analysis strategy is a multi-layered one, in view through research of subtleties and measurable data analysis. This prompts a significant understanding of how cybercrime had been expanding throughout the long term and are there any constraints on Malaysian cyber legislations today. The early piece of the research strategy was an intelligent analysis of my association making study questionnaires and reaching pertinent respondents to help on giving the study connections to accumulate more criticisms. The research on journals, web, articles, and papers on legislations analyses was accessible on material where appropriate. As the result of this data gathering, my chosen methodology became concerned with the available information online and examining the data available. The summary I drew from this chapter and also from the data available, indicated little information on cybercrime's actual reason increases yearly and the cyber legislation's concerns on combating cybercriminals today.

5 Discussion and Analysis

This section surveys two proportions of assumptions, Pearson's relationship coefficient, and Spearman's position, to quantify the outcomes and analysis of data gathered from the

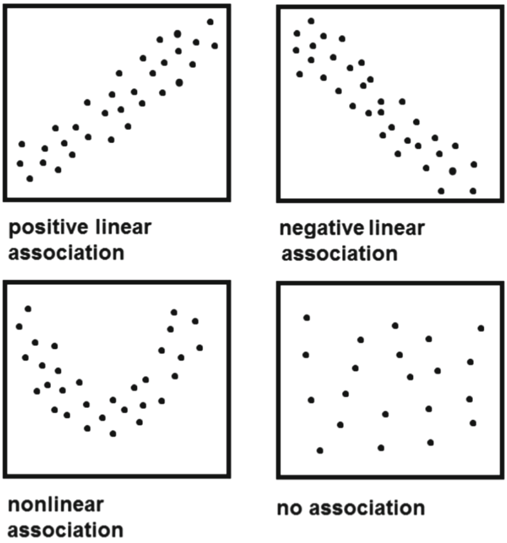


Fig. 2. Scatter Plot of different association

survey questionnaire study. The relationship is introduced genuinely utilizing disperse a plot. Disperse plot is a tool utilized in dominate to distinguish relationships between 2 factors, X and Y. It is one of the seven fundamental instruments for quality control which is valuable while estimating reliance on free and ward factors for a group of data. Disperse plot being chosen to decide if two factors are connected in distinguishing potential underlying driver of the cybercrime increment issue. Different disperse plots affiliation are outlined in Fig. 2. The direct relationship for the most part falls along a line through no-linear will falls along certain bends. Assuming that there is no reasonable sample, this implies no unmistakable relationships between the factors being examined.

The linear relationship can be measured utilizing Pearson's relationship coefficient on the strength and course of the direct relationship between two persistent factors with presumptions. The progressions of 1 variable are related to a difference in another variable, either a certain relationship or negative relationship course. It is utilized on this analysis to decide if expansion in the age, work classifications, and education level are related to the decline in cyber cleanliness practices that prompts the expansion in yearly cybercrimes cases. Data analysis for cybercrime is significant as to decide the underlying driver of expanding yearly cybercrime even though there had been various measures being executed by the public authority yet it doesn't bring down the yearly rate, particularly on cyber extortion cases.

Spearman's relationship estimates the monotonic relationship between two nonstop or ordinal factors where the factors will generally move in a similar relative heading, yet not all the time at a consistent rate. It goes in value from -1 to $+1$. The bigger the all-out worth of the coefficient, the more grounded the relationship between factors.

The study on whether Malaysia law addresses cybercrime effectively, a comparative analysis with other jurisdictions such as the United States (US), the United Kingdom

(UK) and Singapore. All these countries are chosen because of the advanced in both technology and legal framework.

Comparisons of different countries legislations of Malaysia, Singapore, United Kingdom and United State [16, 23–25] which shows that Malaysia cyber legislations are not falling behind comparing with all these countries but instead it does not have a single legislation currently to combat cyber criminals.

Cybercrime	Malaysia Legislation	Singapore Legislations	United Kingdom Legislations	United States Legislation
Hacking (Unauthorised access)	Under Section 3 and 4 of the Computer Crimes Act 1997 (CCA)	Under Section 3 of the Computer Misuse Act (CMA)	Computer Misuse Act 1990	Computer Fraud and Abuse Act (CFAA)
Spam	Under Section 233 of the Communications and Multimedia Act 1998	Spam Act 2003	Privacy and Electronic Communications (EC Directive) Regulations 2003	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, also known as CAN-SPAM Act)

6 Conclusion

Cybercrime develops with the development of technology and these figures show that there should be something lacking either in the analysis, indictment, or the legislation. To accomplish a fruitful indictment in cybercrime cases, Malaysia needs exhaustive new legislation which can arraign cybercrime actually as opposed to having piece dinners of legislation and rules presently. In addition, there is additionally a glaring inadequacy in understanding cybercrime and a gigantic absence of subjective and quantitative data in the experimental parts of cybercrime including the kinds of occurrences, the analysis cycle, and contemporary tool support. This is fundamental towards moulding the planned legislation with thought for the mechanical perspectives [18].

Based on data analytics being studied and reviewed including legislations comparisons with different countries, this shows that Malaysia's cyber security is yet on par with cybercrime growth, especially on cybercrime data. These technologies' changes, it has turned into the impetus for establishing a new refined cybercriminal climate utilizing more development and complex tools to track down their objective casualties. The study uncovers the possible more misfortune in Malaysia because of cybercrime occurrences with the monetary area having the most exceedingly awful hit [17].

Data analytics shows that there are no cyber hygiene practices that lead to yearly cybercrime growth. This study can be a guideline to cyber law enhancement lowering the crime rates. Enforcement is needed to ensure cyber hygiene practices are adopted ensuring at least the first layer of security is in place. Cyber security awareness is to lower cyber fraud by ensuring alertness and minimizing the lack of cybercrime awareness among societies. To accomplish a fruitful indictment in cybercrime cases, Malaysia needs exhaustive new legislation which can arraign cybercrime actually as opposed to having piece meals of legislation and rules presently.

There is still a lack of data in Malaysia ensuring a solid analytics study to prove the findings of cyber fraud increases. Henceforth this research is based on data captured during this research period and analysis by a top to bottom analysis and observational data analysis into different parts of cybercrime in Malaysia with past years' data on fraud cases increases to study on participants' cyber hygiene which can be one of the sources that contributed to increasing in cyber fraud on yearly basis. There can also be another human aspect such as greed, desperation, and others that lure them to cybercriminals as their targets. The result of this analysis can be further enhanced in the future with more extensive study with longer years of data captured for further data analytics.

Acknowledgments. This research is funded by the Ministry of Higher Education Malaysia under the grant no. MMUE/190071.

Authors' Contributions. Swee-Wei Tan: Original draft preparation, Conceptualization.
Kok-Why Ng: Supervision, Reviewing and Editing.
Shereen Khan: Supervision, Reviewing and Editing.
Oliver Swee-Ling Tan: Reviewing and Editing.

References

1. MacTíre Consulting. (2018, October 18). Where does cybercrime come from? The Origin and Evolution of Cybercrime. LE VPN. https://www.le-vpn.com/history-cyber-crime-origin-evolution/
2. Introduction to Cyber Crime http://www.inf.tsu.ru/WebDesign/libra3.nsf/161d3ebc95608f55c62571f5003467e9/3b47f7a6821452fdc62572040016d843/$FILE/cybercrime.pdf
3. Lew, H. (2020, January 29). Why Malaysia Should Amend Its Cyber Security Laws. Asia Law Portal. https://asialawportal.com/2019/11/19/why-malaysia-should-amend-its-cyber-security-laws/
4. Witono, V. (2020, August 30). Machine vs. Machine: Can AI help the cybersecurity skills shortage? GovInsider. https://govinsider.asia/security/machine-vs-machine-can-ai-help-the-cybersecurity-skills-shortage/
5. Mohamed, D. B., Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. Computer Law & Security Review, 29(1), 66–76. 2013. DOI: https://doi.org/10.1016/j.clsr.2012.11.005
6. Rajaendram, R. G. A. (2020, March 21). Lawyers needed for cybercrimes. The Star. https://www.thestar.com.my/news/education/2020/03/22/lawyers-needed-for-cybercrimes
7. 2020 Incident Statistics CyberSecurity Malaysia MYCERT https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=c79b4a49-884f-45eb-94f1-c2826062e039
8. White, T. L. P. W. (2019). MyCERT: Incident Analysis. https://www.mycert.org.my/Portal/Publicationdoc?Id=270d8ee0-Cdd1-49fb-827d-F8fca7752155. https://www.mycert.org.my/portal/publicationdoc?id=270d8ee0-cdd1-49fb-827d-f8fca7752155
9. Statista. (2021, April 7). Malaysia: number of internet users 2015–2025. https://www.statista.com/statistics/553752/number-of-internet-users-in-malaysia/

10. B. (2020, February 11). Gov't actively addressing cyber threats, crimes - DPM. Malaysiakini. https://www.malaysiakini.com/news/510476
11. Qualitative, quantitative and mixed methods dissertations | Getting started with Lærd Dissertation. (2012b). Laerd Dissertation. https://dissertation.laerd.com/getting-started-p2.php
12. Ibrahim, R., Understanding Cybercrime in Malaysia: An Overview. 2014 https://www.academia.edu/28931735/Understanding_Cybercrime_in_Malaysia_An_Overview.%20https:/www.academia.edu/28931735/Understanding_Cybercrime_in_Malaysia_An_Overview
13. Global Legal Group., Cybersecurity 2021 | Laws and Regulations | Malaysia | ICLG. International Comparative Legal Guides International Business Reports. 2021. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/malaysia
14. Printful. 2020. https://www.printful.com/Blog/the-Basics-of-Ecommerce-Fraud-What-Is-It-and-How-to-Manage-It/.%20https:/www.printful.com/blog/the-basics-of-ecommerce-fraud-what-is-it-and-how-to-manage-it/
15. U. (2017b, July 26). Malaysian Public's Concern About Cyber Security Issues Escalates. Unisys. https://www.unisys.com.my/offerings/security-solutions/news%20release/my-malaysian-public-concern-about-cyber-security-issues-escalates
16. Malaysian Bar. (2015, April). Joint Press Release | Amendments to the Sedition Act 1948 are Draconian, Militate Against the Freedom of Speech and Expression, and Interfere with the Independence of the Judiciary. https://www.malaysianbar.org.my/article/news/press-statements/press-statements/joint-press-release-amendments-to-the-sedition-act-1948-are-draconian-militate-against-the-freedom-of-speech-and-expression-and-interfere-with-the-independence-of-the-judiciary
17. Rahman, R. (2019). CYBERCRIME CASES IN A DECADE: THE MALAYSIAN EXPERIENCE. Independently published.
18. Kuala Lumpur, MalaysiaShearn Delamore & Co. (2015). Laws of Malaysia with Commentary. Thomson Reuters. https://www.shearndelamore.com/pdfs/Thomson%20Reuters-%20World%20Intellectual%20Property%20Rights%20and%20Remedies%202015.pdf
19. LGMS. (2021, May 20). Best Computer & Digital Forensic Services in Malaysia | LGMS. LGMS - Penetration Testing (Pen Test) Expert Malaysia & Asia. https://lgms.global/digital-forensics/?gclid=EAIaIQobChMI6_T97KSm6gIVUQ4rCh2v-wJREAAYAiAAEgL0oPD_BwE
20. Haukilehto, T. (2019b). Improving Cyber Security awareness: Health, social services and regional government reform in South Ostrobothnia | Semantic Scholar. Tero Haukilehto. https://www.semanticscholar.org/paper/Improving-Cyber-Security-awareness%3A-Health%2C-social-Haukilehto/03205602e412a5d91246a373dd9694905a700eed?p2df
21. Eschelbeck, G. (2000). Active Security—A proactive approach for computer security systems. Journal of Network and Computer Applications, 23(2), 109–130. https://doi.org/10.1006/jnca.2000.0103
22. Malay Mail. (2020, January 7). Malaysia sees improvement in cybersecurity awareness. Malaysia | Malay Mail. https://www.malaymail.com/news/malaysia/2020/01/07/malaysia-sees-improvement-in-cybersecurity-awareness/1825545
23. Global Legal Group. (2021a). Compare & Research | Cybersecurity | ICLG. International Comparative Legal Guides International Business Reports. https://iclg.com/compare/cybersecurity
24. Yik, C. S. (2021b, April 8). Basics of Cyber Security Law in Malaysia. Chia, Lee & Associates. https://chialee.com.my/basics-of-cyber-security-law-in-malaysia/
25. The Effect of Section 114A of the Evidence Act 1950 on Internet Publications | Thomas Philip Advocates and Solicitors, Kuala Lumpur, Malaysia. (2019c). Pauline Lim Wenjun. https://www.thomasphilip.com.my/articles/the-effect-of-section-114a-of-the-evidence-act-1950-on-internet-publications/

26. Mok, O. (2021, February 19). MyDIGITAL and Malaysia Digital Economy Blueprint: How we can achieve 100pc internet access. Malaysia | Malay Mail. https://www.malaymail.com/news/malaysia/2021/02/19/malaysia-digital-economy-blueprint-how-we-can-achieve-100pc-internet-access/1951007#:%7E:text=The%20Malaysia%20Digital%20Economy%20Blueprint%20will%20be%20implemented,regulatory%20framework%20that%20can%20expedite%20digital%20infrastructure%20development.