INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

The Influence of New Media on Cybersecurity and Law Implementation: A Qualitative Study

Nul Widaya Mohamed Nawi, Syed Agil Alsagoff, Mohd Nizam Osman, Zulhamri Abdullah, Nur Shuhamin Nazuri

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v12-i6/13863 DOI:10.6007/IJARBSS/v12-i6/13863

Received: *18* April 2022, ***Revised:*** *20* May 2022, ***Accepted:*** *04* June 2022

Published Online: *15* June 2022

In-Text Citation: (Nawi et al., 2022)

To Cite this Article: Nawi, N. W. M., Alsagoff, S. A., Osman, M. N., Abdullah, Z., & Nazuri, N. S. (2022). The Influence of New Media on Cybersecurity and Law Implementation: A Qualitative Study. *International Journal of Academic Research in Business and Social Sciences. 12(6),* 944– 961.

Vol. 12, No. 6, 2022, Pg. 944 – 961

http://hrmars.com/index.php/pages/detail/IJARBSS | **JOURNAL HOMEPAGE**

Full Terms & Conditions of access and use can be found at
http://hrmars.com/index.php/pages/detail/publication-ethics

INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

The Influence of New Media on Cybersecurity and Law Implementation: A Qualitative Study

Nul Widaya Mohamed Nawi[a], Syed Agil Alsagoff [a], Mohd Nizam Osman[a], Zulhamri Abdullah[a], Nur Shuhamin Nazuri [b]

[a]Department of Communication, Faculty of Modern Languages and Communication, Universiti Putra Malaysia, Serdang, Malaysia, [b]Department of Social and Development Sciences, Faculty of Human Ecology, Universiti Putra Malaysia, Serdang, Malaysia
Corresponding author Email: nul_widaya@yahoo.com

Abstract

This paper aims to provide an explanation the influence of new media on cybersecurity. Through the Media Dependency Theory lens, researcher can see the use of new media from a media perspective where the media plays a role in this society. This paper describes the influence of new media on cybersecurity and law implementation in Malaysia. The researcher conduct focus group discussion for this paper. Focus group discussion is a qualitative research technique that involves conducting intensive group around 4 groups with six persons each group until get the saturation data. This small number of informants is to explore informants perspectives on a particular idea and situation. Analysis document also use as approach to analyse the law implementation related cybersecurity. The findings of this study identify new media dependency, namely impact of new media and the influence of new media that related to the cybersecurity. In addition, the study highlights about the law implementation in Malaysia. This paper provides a comprehensive critical picture of the growing new media usage literature and information that offers the basis for a comprehensive assessment of new media usage contributions to people in particular and enhances relevant knowledge new media.

Keywords: New Media, Media Dependency, Cybersecurity, Law Implementation

Introduction

The new media has created a single world culture nowadays. New media is a popular platform for people to change information, share their ideas, thoughts, opinions, photos and videos using well-known websites and social messengers. Generally, users access new media with the help of technology while providing the right environment for people of different age groups to interact and connect with each other, new media and messengers are effective tools for providing opportunities. However, new media has become a necessary and important tool for the Malaysian community, especially the youth in Malaysia. Besides, the new media is more popular because its role in disseminating information without limits.

This paper is importance to be conducted because it can provide the latest information as well as to be a complement of previous studies. In addition, as a country without Internet censorship policies shall adopted the aspects of awareness and security practices in virtual world. Through this study may explore the weakness of cybersecurity practices in Malaysia and able to come out with a solution/recommendation to the government. Those recommendations are obtained from the Authority such as government staff and the consumers of Internet itself. This is because, they possess much more understanding of the problem and would be able to suggest the best solution in dealing with the problems. Apart from that, this study can provide an information to the government to not or enacting a special act pertaining of the Internet abuse.

The enactment of cyber special acts often becomes a debates issue among academics and politician as resulted from the increase of cyber cases. Therefore, through this study can explore the need of the existence of a new cyber act in Malaysia. Non filtering or censorship of Internet policies in Malaysia may impact to the increment of cybercrime among society. Up until now, government are yet to established any special act to control the Internet abuse (Markom et al., 2019). Thus, the government shall emphasize the element of selves control to be carried out by individuals, organizations or the parents. However, the question is to what extent does the user aware to prioritized the aspect of safety while making any transaction through new media technologies. Unfortunately, the level of awareness among Malaysian are still at lower level and thus exposing them to easily become a victim of cybercrime (Jerde, 2017). Therefore, the result of the study may pinpoint the Internet users on the awareness and the safety of surfing Internet. Furthermore, this paper can educate public about acts, regulations and law of communication including codes content of Internet. The theoretical perspective can be enriched by conducting the study especially the Media Dependence Theory introduced by Sandra Ball Rokeach & Melvin DeFleur 1976 (Jiang et al., 2018). Moreover, this paper can become a references in academic field as it's enriched with theoretical perspective. The dependency between the theories possible to generate and organize ideas by creatively and neatly. In addition, through theories provide a good explanation towards the key point of the study. By the mean of those theories shall be giving a depth understanding on the phenomenon of cyber security practices as to much dependency towards new media cause the user vulnerable to cyber threats. Therefore, cyber security practices need to be placed by several components that influence their practices i.e. awareness, social environment, experience and law (Aarssen & Crimi, 2016). This could determine the changes towards user behaviours in the cybersecurity practices. Methodology is the center of the research study. The use of proper and correct methodology can produce reliable data with quality. Therefore, this study would use a qualitative method in answering the research question of this study. Qualitative analysis method can provide a useful research material especially towards the cyber security in Malaysia.

Digital identity is expected to become a major issue in the future as society balances between preserving online privacy and providing protection against fraud and online crimes. According to Internet Users Surveys (2020), 88.7% of the population are Internet users in 2020 1.3% increase from 87.4% in 2018. The Internet Users Survey (IUS) is a series of purpose-built surveys conducted since 2012 to monitor Internet activities and understand the trends and tendencies among users. Consequently, the surveys have provided stepping stones thus far, to gauge Malaysia's standing in Internet adoption in recent years. Based on a statistical report

released by the Cyber Crime Investigation Division and Multimedia PDRM, a case of telecommunication fraud by online and SMS is the higher total of losses that also the number of youths that involve in this matter is highly increase. Table 1 and 2 below showed the statistic of victims in 2020 and type of telecommunication fraud.

Table 1
Statistic of victims in 2020

Age	Malay		Chinese		Indian		Others		Total		
	Female	Male	Female	Male	Female	Male	Female	Male	Male	Female	
15-20	363	324	146	125	47	39	51	45	607	533	1,140
21-30	962	1,193	609	708	139	167	229	237	1,939	2,305	4,244
31-40	803	953	519	637	136	100	167	182	1,625	1,872	3,497

Table 2
Type of telecommunication fraud

	Total of IP	Total of Losses
Fake News	0	-
Personal Data Protection	12	RM 449,547.70
233 AKM (Social Medial)	48	RM 15,702.48
Telecommunication Fraud (Online/SMS)	5,998	RM 287,298,685.91
E-Financial Fraud	662	RM 25,635,220.69
419 Scam (Love Scam)	1,582	RM 58,335,797.29
E-Commerce (On-line Purchase)	5,847	RM 41,332,618.48
Intelectual Property (CD/VCD/DVD)	19	-
Pornographic Material (Sek 292 KK)	49	-
Total	**14,205**	**RM 412,618,024.85**

Cyber Crime Investigation Division and Multimedia PDRM (2020)

Social Environment and Cyber Security Practices

Social environments such as government policy, peers, mass media, role of parent plays an important role in determining cybersecurity practices. Government policy in tackling cybercrime is one of the example. To improve awareness among new media users, the government has launched the Safer Internet Day program in the year 2010 (Fleming-Milici & Harris, 2020). It aims to encourage people to use Internet by prudently and ethically. In addition, the government also provides exposure to the public, especially youth on how to use new media safely and positively (CyberSecurity Malaysia, 2020). As a government effort towards creating awareness to the community, the concept of mentor-mentee was also introduced through this program.

Furthermore, in March 2016, the Ministry of Domestic Trade,Cooperatives and Consumerism have submitted proposals regarding the individuals whom selling goods privately need to register a business with Companies Commission of Malaysia. This is due to the increase of online fraud purchase cases been reported. According to Marimuthu (2016),

cases of fraudulent purchase of internal goods was the highest in 2015 by recording losses in excess of RM4.9 million among the sectors involved automobiles, housing and tourism. In addition, scholars in the cyber security field also suggested that the government should introduce a special syllabus on cyber security at the school level especially in primary schools. This is because the existing subjects do not cover aspects of cybersecurity fully and only focuses on the fields of computers and multimedia. These recommendations should be taken into considerations in determining the cyber security practices of Internet users.

From the aspect of parents, a study was conducted by Anita (2016) on the relationship between parenting style and Internet use. This research was conducted by 350 school children around Putrajaya with using of the questionnaire method. She tested three methods of maternal monitoring style i.e. authoritative, permissive and authoritarian. The results show the authoritative style monitoring is the most frequent used by parents. He also recommended parents to use a permissive monitoring style such as using the Internet with children, assigning related Internet tasks and discuss with children about Internet content. Besides that, parents can obtain more depth knowledge through the Click program With Bijak organized by SKMM as stated above.

According to Adnan (2013), in addition to social environment factors, there are several other factors that drive cybercriminals to commit such offenses. This is because the criminal considers themselves difficult to identify by the authorities. Besides, from the point view of criminals, the government is not able to carry out content monitoring on a regular basis. In addition, the criminals use domain or web hosting from abroad where it is difficult for the government to obtain the identity of the criminal. Cybercrime is not an issue and considers not necessary to be noticed by any party. If the awareness factor is still lacking in the society then the probability the number of cyber cases in Malaysia to increase. Therefore, awareness measures in the issue of cyber need to be exposed to all layers of society in order to curb and reduce cyber crime cases in Malaysia.

Data Analysis

Once the data is obtained from the informant, data analysis for focus group and interview methods, the data obtained through video and MP4 recording has been converted into text transcription. Data analysis was performed as soon as the interview with the informant was completed performed. This allows for comparisons and notes between one group with other groups. Data were also analyzed using NVivo software to obtain accurate data. Besides, it is too make it easier to manage making or determining the themes in this study and maintain the confidentiality of the study informants then each informant in the focus group given labelling to facilitate the process of writing the results of the study. Table 3 below showed the focus group informant labelling.

Table 3
Focus Group Informant Labeling (KF)

Focus Group	Informant Number	Informant Labelling
1	6	KF1-KF6
2	6	KF7-KF12
3	6	KF13-KF18
4	6	KF19-KF24

Results and Discussion

The Role of the New Media

The new media has a key role and responsibility in development a country. This is because all information will be channeled to the public and outsiders through mass media such as electronic media and print media. Mass media are also seen as the power to control and change behavior as well perceptions of an individual, a community or even society. In determining cyber security practices, the media needs to be used as effectively as it is as well impacting the development of the country.

Thus, among other issues raised by the informants is the role of the mass media in providing cyber security awareness among new media users. Malaysia needs further improvement in cyber security so that the community is more clear and visible towards media responsibility. Accoridng to the informants, not all media in Malaysia covers about cyber security. Informants such as KF3, KF10, KF31 stated that the press is more responsible in featuring issues on security cyber compared to electronic media. KF1 informants also stated he was just looking at the role of electronic media in TV1 versus the electronic media others such as TV3, TV9, TV8 and so on. This is because TV1 used to make coverage and publication of issues related to safety awareness and practices cyber in Malaysia. This is supported by the statements of the informants as follows;

KF1*: ... this existing role needs to be enhanced again..if we look at it, there are usually a lot of cyber articles on TV1. Other channels also have to play a role..not hopefully on TV1 right.*

KF3*: ... I also agree… Other TV shows don't seem to promote this cyber security article. In ordinary papers, they report on cyber cases.*

KF10*: ... near the regular newspaper I read the news about cyber crime, like in the daily news to ... on TV I rarely watch.*

KF31*: ... if the role in the newspaper is like the daily news, it seems that the usual daily news reports on cases of alleged violations or cyber defamation.*

The media only reported on aspects of cyber security but no initiative from the media to conduct cyber security awareness campaigns or programs for the user. Media mostly focus on exclusive programs such as carnivals and so on. Furthermore, the media only be looking for cyber security agencies when the media needs help from them. This matter can be seen as the statements of the following informants;

KF98*: ...media only approach us when something that need expertise on.*

In addition to the above, mass media does not play a full role in cybersecurity issues. The media tend to choose issues that have news value. In addition, the government has to incur high costs to get broadcast or advertising cyber security in new media. In this case, the media shall play the role to focus also on I cyber security as a societal issue and it needs to be made as the corporate social responsibility of the mass media. This is stated by the informants as follows;

KF113*: ...hurmm campaign one of the reasons that quite expensive in media electronic. so we prefer to do a simple video and upload on YouTube.*

***KF99**: ... the choosy media, he will choose cases that involve more great value and also recurring cases.*

Thus, to further enhance the role of the mass media, the study informants also suggest some steps that can be practiced by the media. Mass media such as electronic media should provide special broadcasts for cyber security issues such as the 999 show on TV3 or the broadcast on *Selamat Pagi Malaysia* or Women Today. In addition, the media also needs to issue films or dramas related to cybersecurity. In addition to using the stories of Upin and Ipin in giving awareness to children about cybersecurity. In addition, the informant also stated the media need to conduct cyber security awareness campaigns and programs and this because media -organized programs do not require costs for broadcasting and can using their respective channels to make a fuss and spread the word such programs. This is evidenced by the statements of the informants following;

***KF18**: ... there should be special slots for this cyber crime. An example of a 999 program*

***KF21**: ... the media itself went down to the field to campaign on how to get closer to the community, I think it works better ... and there is no need for broadcast costs.*

Overall, these findings suggest that the role of the mass media in Malaysia in terms of cyber security needs to be further improved so that it benefit the community and the development of the country. Besides, the mass media also needs to make the issue of cyber security a societal issue in addition as a mass media corporate social responsibility.

Government Policy

For a developing country like Malaysia, government policy needs to play a crucial role in leading the country. Government policy will determine the direction of a country. Generally, government policy refers to a guideline and planning on a clear goals and valuse issue. Besides, a policy created to solve a critical problem happening in a country. Somehow, the policy is comprehensive by taking into account various views and aspects. Thus, in addressing the issue of cyber security threats, three government policy proposals that submitted by various parties are also taken into account in this study such as private online sellers need to register with the Commission Syarikat Malaysia (SSM), the existence of cyber security education syllabus and the existence of cyber courts.

The results showed that the informant mostly agreed for the government to implement the policy. This is because, with the existence of this policy can directly protect the rights of users. Although however, the government needs to refine the implementation of this policy by taking various factors such as taxation and so on so that it not to the detriment any private sellers. This is supported by the statements of the study informants as follows;

***KF22**: ... I agree if the government wants to do it but there must be a clearer explanation from the government such as taxes, who has to pay, that's how it is.*

***KF33**: ... the government's good proposal to register but there is no explanation because people are worried and come out with all sorts of speculations ... I personally agree with the implementation of this thing.*

In addition, a discussion of a special syllabus of cyber security shall be held at school level and university. This is because the informant stated the government had introduced the subject of Information and Communication Technology (ICT) for grades 4, 5 and 6 of primary school. However, the government needs to improve the subject. This is because, by this subjects students are exposed to how to create documents, download songs from the website to student files and documents but students do not taught about copyright like having to put resources when copying something or download copyrighted songs and so on. This is supported by the following informants;

TM36*: ... now taught how to copy but they need to understand be cannot copy fully, copy you need to use technoloy so that is certain ethic aspect of the copyright why you cannot download music, the ethic aspect may be a little lacking I think. But the technical part ... I think the co-curriculum, example how to do a document, excel, calculation in excel. the technical aspect is yes. but you have to look one step further at ethic aspect because its including to building in social engagement ... when you do script writing, let say you write any script writing, you must learn to respect others copyright or when you do literature you need to respect the article part, you just doesn't apply, you just need to respect copyright, do not take Wikipedia only, that sort of things, we should learn the knowledge.*

In addition, the informant also stated that aspects of cyber security can be taught through existing subjects. For example, under the subject of Language Malay, students can be given an essay entitled cyber security. Besides, the topic of cyber security can be used as a discussion in class or through competitions such as speeches as well as cyber security awareness weeks. This matter evidenced by the statements of the following study informants:

KF17*: ... I don't think it is necessary, maybe in the cyber aspect, we can include in civic education, we can insert as an additional subject that seems inappropriate involving teachers*

KF29*: ... enter while cross -curricular, no class required. For example, make a discussion about the problem in a speech*

KF30*: ... not necessary. It can only be included in the subtopic of computer use ... the computer usage syllabus does not need to be long for students and diversify the syllabus by including the aspect of cyber security.*

KF31*: ... cyber security awareness is important because teenage girls aged 13, 14, 15 are always sexual victims in cyberspace. So, maybe there is no need to make an effort to create a special subject but like you said earlier, across the curriculum maybe we can try to implement that thing. Because awareness is important.*

In addition to those issues, on September 1, 2016 the government created a court for cyber specialty operating in the Federal Territory of Kuala Lumpur. Hence, the issue on the establishment of a special cyber court was also submitted to the informants of the study. The results of the study found that the average informant agreed with the establishment of special cyber courts due to the increase in cyber crime cases in Malaysia. In addition, the informant stated that there is a special court this cyber it facilitates the trial process to run smoothly and quickly. In addition, the informant also stated that in the presence of this court, the party

judges and lawyers can delve into technical issues and it simplifies the process prosecution. However, this establishment requires capacity, logistics, sources and so on. This can be seen based on the statements of the informants following;

KF1*: ... this one needs to be seen for the long term. We also don't know how the New media will develop in the next 10 years. There must be many more cyber crime issues, so this court is really good.*

KF42*: ... in my opinion we should because discussion in term on cyber security or cyber IT or related issues.It is needs to be to be discussed somebody who knows about the technical and knowledge, we need technical knowledge you don't understand how ip works, how content content of information ... how do you want to understand one case at a time so the magistrate is the one who makes the decision, the judge must have information, there must be at least knowledge than the prosecutor, everything must be understood as well so that you can make proper decision, so i think with cyber court we have proper judge we have to build capacity… Proper knowledge about information security, about network works, how prosecutor lawyers can understand i think we could have law kind of cases that we can solve… because nowaadays some cases do not have any action, and lot of it, because maybe the prove not enough.*

Based on these findings, it can be concluded that the average informant argues that government policy plays a major role in determining the cybersecurity practices. Besides, the government shall practices and recommended in the implementation of registration policies by sellers of goods alone with the existence of cyber courts as it can define positive cybersecurity practices in the circles of New media users. In addition, the informant also stated that the government should make improvements in the primary school curriculum especially in subjects Information and Communication Technology so that students are exposed earlier about cybersecurity and being able to protect them from cyber threats.

The influence of peers found did not play a role in helping the informant to improve on their cybersecurity practices. The third is the role of the workplace, the study found the workplace of the informant studies working in the private sector did not play a role in improving cybersecurity practices because of the average informant working in private is not disclosed about any cyber security activities in place their work. Moreover, for the fourth factor which is the role of the mass media, the result it can be concluded that most of the informants stated the role of the mass media in Malaysia in terms of cyber security needs to be further improved so that it gives benefits to society and national development. For the last factor that is government policy, the results can be summarized that the informants agreed and supports government policy in the registration of online sellers in the Companies Commission Malaysia and the implementation of a special cyber court because informants are confident it can bringing positive cybersecurity practices among new media users.

Law Enforcement on Cyber Security Threats

This section describes the results of the study findings through document analysis on Malaysian law and cyber security threats. This part also answering the fourth objective of the study which is to analyze the implementation of laws on cyber security threats.

Powers and Implementing Bodies in Controlling Cyber Security Malaysia

The term power is often associated with the political world with government. In a power state is very important in determining policies and regulations against something. This is because of the power of an individual can make decisions as well as control the behavior of others. Power too making an individual or organization stronger. Generally, an individual as well as an organization will gain power through allocation the law of a country. Thus, power is also very much needed by the body cyber security implementers so that their role is broader and can act comprehensively in controlling cybersecurity. Therefore, the results of the analysis the document finds, based on two implementing bodies key that has the power in controlling cyber security Malaysia namely Malaysian Communications and Multimedia Commission and the Royal Malaysian Police.

Cyber Law Implementation in Malaysia

In general, law refers to a norm and system of rules which is used to control the behavior of a society. Normally, the law consist a set of punishment according to an offense performed by an individual. Meanwhile, cyber refers to an acts or communication activities by using computers and the new media. Thus, cyber law refers to the rules and penalties associated with the communication activities via the new media using digital communication devices. The results of document analysis found that in Malaysia there is no term for cyber law. However, it does not mean there are no laws in ensuring Malaysia's cyber security. This is because, the result studies show there are several traditional and existing laws that can be applied to control cyber security threats. Existing law can be used to enforce the above sentence offenders because the new media is a medium or platform used for communication.

Communications and Multimedia Act 1998

The act is enforced by the Malaysian Communications and Multimedia Commission. It’s contain a total of 282 of sections relating to cyber security which are section 211 and section 233. Based on section 211 (1) an individual or content application service provider may not provide content that is indecent, obscene, false, threatening or is ugly for purpose and intent to harass, abuse or threaten anyone. Based on this provision it is clear that such activities as cyber bullying, pornography, transmitting viruses, spreading slander or even fake news are an offense under this section and in the event of a contravention of section 211 (1) then may be subject to a fine and imprisonment under section 211 (2) which is a fine not exceeding fifty thousand ringgit or imprisonment not exceeding a term of one year Next, for the user of WhatsApp, Telegram or WeChat groups may be subject to action if they commit an offense as provided in this section. Besides, its also applied to an individual who has committed an offense of sharing, retweet, forward to the offending conten. For example, Hussein made false statements on his Facebook, and Ahmad as Hussein's Facebook followers also share the information on his Facebook site. In this case, under section 211 Hussein has violated the rules for supplying fake content through Facebook and Ahmad has also committed the same offense because of his act in shareing the original content supplied by Hussein.

In addition, the results of document analysis found that section 233 provides for offenses on the misuse of network facilities or network services. Based on this section one cannot use the network to make or send any comments, requests, suggestions or obscene

communications, fake, incestuous, and threatening with intent to harass others may be liable to a fine not exceeding RM 50, 000 or to imprisonment not exceeding 1 year or both.

Computer Crimes Act 1997

This act is an adaptation of Computer Misuse Act 1990 United Kingdom which has been adopted by Malaysia. The purpose of the enactment of this act is to provide for offenses in computer abuse (Rahim & Manap, 2004). The Act consists of three main parts and 12 sections. Pursuant to Section 3 (1) in emphasizing more on offenses related to computer misuse with intent to make access without authority. For example, someone who does not have permission from the computer owner has turned on the computer system and download some information from the system onto a diskette (Rahim & Manap, 2004). According to Section 3, the said person have done something wrong if;

(a) causes a computer to perform any function with intent gain access to any stored programs or data in any computer;
(b) the access he intends to obtain is without authority,
(c) he knew the caused of the computer to perform such function.

This section consists of two important things i.e. necessary where there is an intention to gain access to any program or stored data in the computer and both accesses are without power (Rahim & Manap 2004). If convicted the offense may be charged of not exceeding RM50,000 or imprisonment not exceeding 5 years or both.

In addition, the results of document analysis found, there is four (4) sections states an offense of unauthorized access. However, these sections only applies when there is an offense under section 3 above. Therefore, this is difficult for these 4 sections to be applied to the prosecution process. For example, Ali transmitted a virus to Ahmad's website which is open to the public by using own computer. In this case, even Ahmad suffered the loss due by the virus but Ali cannot be prosecuted because achievement without power does not exist there because Ali uses his own personal computer. Weaknesses in this section need to be rectified as suggested by Rahim and Manap (2004) as follows;

“A person is guilty of an offense under this section if he:

(a) commits an offense involving fraud or dishonesty or which causing injury as defined in the Code of Punishment; or

(b) facilitates the commission of an offense either by himself or by any other person. ”

c) Electronic Commerce Act 2006

This act protects consumers in online business. Under section 5 of the interpretation, commercial transactions means a one -way or multiple communication of a trade nature, whether contractual or not, includes any matter of relating to the supply or exchange of goods or services, agencies, investment, finance, banking and insurance. The user able to conduct transactions in a more guaranteed environment. However, the results of the study found that this act through section 3 (1) states that use is not mandatory as follows;

"3. (1) Nothing in this Act shall make it mandatory for a person to use, give or receive any electronic message in any commercial transaction unless that person consents to the use, giving or receiving of such electronic message. "

Based on the statement of informant KF97, the purchase of goods is under civil action and the Electronic Commerce Act 2006 but not included under criminal acts. The traders still have a choice of either to be subject under the Electronic Commerce Act 2006 or under the Contracts Act 1950. This is because the Electronic Commerce Act 2006 among merchants is optional. Thus, non -mandatory provisions in the Electronic Commerce Act 2006 are necessary revisited because if a trader uses his business dealings by electronically. Unfortunately, to follow or not the Act Electronic Commerce 2006 raised the issue of conviction in court in the event of elements of fraud and so on.

KF97*:… The purchase of goods is a civil action and this deed is not mandatory. For example, when I do business, I can choose whether I want to be under this act or not or whether I want to use the normal Contract Act 1950 only. This means that I as a trader can clearly state that my business is not covered under the Electronic Commerce Act 2006.*

d) Digital Signature Act 1997

The results of the document analysis show that this act also emphasizes confidentiality in enclosing confidential information. If founding guilty, an offense under section 72 and may fined not exceeding RM 100, 000 or imprisoned for not exceeding 2 years or both. Besides, if someone is making any false information can also be convicted of an offense under section 73 and carries a fine not exceeding RM 500, 000 or imprisonment for a period not exceeding 10 years or both.

e) Personal Data Protection Act 2010

Advancement in ICT can nolonger guaranteed privacy. Nowadays, there are handful of local companies or irresponsible people who misuse one's personal data especially commercially. So, on June 10, 2010 Data Protection Act Personal 2010 was introduced. The findings indicate the main purpose of the enactment of the act is to regulate the processing of the personal data of the individuals involved in commercial transactions and online transactions. The results of the analysis show the act containing 11 sections which has seven principles that one must adhere to. First, the general principle of where a user is not allowed to process other person's personal data without authority. Second, the principle of notice and choice where data users need to inform the initial purpose to the data subject. Third is revelation. This means the purpose of a subject's personal data is in order to identify the meaning for the personal data is to be disclosed. Next is safety where processing od data and necessary steps taken for th safety of data, not modified, misused or given to parties who are not concerned.

Then, is the principle of storage. Personal data is not allowed to be stored in a processing beyond the required time limit. The sixth is the principle of data integrity where every personal data is ensured to be accurate, complete, not confusing and up to date. The seventh is the principle of access where a person shall be given the right of access to his personal data held by a user of the data and can also correct the data so that it is up to date.

Moreover, the results of the study found that an individual has the right to prohibit their personal data for commercial or marketing used. This can be done by giving written notice to the data user. This act is under the provisions of section 43 (1). According to section

43 (2) if the data user still refuses to comply with the notice then the individual can make an application to Commissioner to require the data user to comply with the notice. If the data user still fails to comply with the notice, then can be convicted under section 43 and in accordance with section 43 (4) may carry a fine of no exceeding two hundred thousand ringgit or imprisoned for a term not exceeding two years or both. In addition to the above, according to section 129 (1) (2) (3) a person's personal data also cannot be transferred outside of Malaysia unless with the consent of the individual or involving a contract. If he fails to comply with this rule then according to section 129 (5) can fined not exceeding three hundred thousand ringgit or imprisoned for a term not more than two years or both.

However, based on the statement of informant KF44, this act is for commercial purposes. Any party conducting commercial affairs need to register with the Personal Data Protection Department. If the data is not for commercial purposes, then not necessary to be registered at the relevant department. For example, an NGO's personal data of students throughout Public Universities in Malaysia. The question is whether it is necessary to register with the Personal Data Protection Department. However, in this situation, what if the data owned by NGOs have been invaded or stolen by others? Of course it will cause various problems. Therefore, in this act should be included once non -commercial so that the data obtained can be managed securely. This can be seen through the following statement of KF103 informants:

KF103:*… he applies to parties who do commercial business only if it is not commercial he does not need to register. For example, I am an NGO. I keep the personal data of all IPTA students so I do not need to register with the Personal Data Protection Department because I am not a commercial.*

f) Sedition Act 1948 (Amendment) 2015

Sedition offenses not only involved in print media but also happens on the new media such as through social sites, blogs and others. Thus, the Sedition Act 1948 was enacted. Although this traditional law was enacted in 1948 and has been amended several times including in 2015 and as a reference to address the issue of sedition through New media. Section 4 (1) (1A) is one of the appropriate sections to deal with sedition through the cyber world. The findings of the document analysis show, if a person has a tendency to incite or mention any inciting word would be fouding guilty. Besides, it would be an offense of an act of print, publish, sell, offer for sale, distribute or reproduce any seditious publication. Anyone who violates the this provisions, then pursuant to section 4 (1) shall be liable to imprisonment of not less than 3 years and not exceeding 7 years and pursuant to section (4) 1A may be imprisoned not less than five years and not more than twenty years.

g) Defamation Act 1957

Defamation issues in new media such as Facebook, Twitter and so on has became trending among new media users. Kent & William (2006) stated that defamation can be categorized into two which are libel or slander. Libel is defamation through newspapers, memos issued between offices, books, movies, sites web, music and so on. While, slander is through spontaneous or through force movement. Therefore, the results of document analysis found that the Defamation Act 1957 was also being adopted to protect those who have been defamed through websites and the new media. For example, in the case of plaintiff v defendant the court also referred to Section 8 of the Defamation Act 1957. For example, the

defendant had published in his blog of an article of the rape case under the heading "Hey Mr. … where do you want to walk…" with a photo of the Plaintiff. Defendant defended himself by saying that the article was cited from the website and he just republished the article mentioned in his blog. However, the court found he was not only copied and pasted the article but included also a picture of the Plaintiff in the article. This causes the defendant to have added facts from the original text. Therefore, the court has decided on compensation damages of RM 300, 000 to the Plaintiff.

h) Printing Presses and Publications Act 1984 (Amendment) 1987

Based on the results of document analysis, it is an act enacted to control the issuance of printing press licenses and publication permit. The Act also protects against any party from publishing news that is not true and this includes fake news in the new media. This is evidenced through case of plaintiff v. defendants. This case is referred to under Section 8A, Printing Presses and Publications Act 1984. Defendant has republished an article from an MP's blog which illustrates that Plaintiff has the ability to distort surahs of the Quran for its own political purposes. Defendant defended himself by stating that the article does not make any direct reference to the plaintiff and instead of slandering him. However, the court ruled the defendant was guilty because the second defendant did not make any attempt to confirm the accuracy of the article and also does not make any denial to the reader that the article is a view from the MP's blog. Therefore, the court allowed the plaintiff's claim with damages of RM70,000.

Furthermore, it has been made clear under the provisions of section 8A stating then the printer, the publisher, editor and writer of the news would committed an offense if the published publication contained of malicious intent. This offense carry a prison sentence not exceeding three years or a fine not exceeding twenty thousand dollars or both. However, in the context of a person's online publication needs to be proven that individual concerned had malicious intent prior to prosecution. Despite this act applies to errors on the new media but there needs to be improvement in terms of publication definition details. This is because under section 2, the definition of publication is unclear about electronic publishing. Publication here means a document, newspapers, books, periodicals, all written or printed materials as well as anything else which according to its appearance, form or in any way can imply words or ideas. Therefore, the element of online publishing needs to be included inside the definition of publication under this act so that it is clear and simplifies the process of prosecution in court.

i) Copyright Act 1987 (Amendment) 2012

The Act was gazetted on 21 May 1987, amended in 2012 by repealed the Copyright Act 1969. The results of document analysis found, this act protected work such as literary works, music works , artwork, photographic works, films or sound recordings as well as broadcasts transmitted from within any country. The law also protects the work on the new media. According to Shamsul (2008) copyright is not intended to protect the thoughts or ideas created by the author or but only in a way of its delivery. Copyright protection in Malaysia exists automatically when a work is produced. This automatic protection also includes internal works through The New media is in the form of digital and graphics (Shamsul, 2008). Any data stored on a computer's hard drive will be considered dated something that work is produced. According to him, the activity of downloading music, movies, games or software from the new media are also protected under the Copyright Act. However, there are also some websites

that allow the activity for free downloaded without copyright infringement. Section 3, defines a copy as a reproduction of work in the form of writing, recording, film or in any form of another material. Thus, literary works for example, can be published in book form, recorded or even entered on the new media (Shamsul, 2008).

j) Evidence Act 1950 (Amendment) 2012

This act has been amended several times from the Year 2012 with the provision of a new section of 114A. By the existence of section 114A simplifies the control of offenses on the new media. Based on the provisions in section 114A, it can be found that all publication or action is the responsibility of each. This matter means users should always be vigilant when using the new media. By analogy, Section 114A (1), Ahmad uses Siti's picture in his blog as a profile picture. Apart from that, Seri has published a defamation article while, Siti will have to published the article. Another analogy is when Seri has WiFi line service, and Siti has hacked the WiFi to published the article but considered published by Seri. The third analogy based on Section 114A (3) Seri has a laptop and coincidentally his Facebook social site iopen and Siti has broken into the laptop and published something comments with seditious elements on Ahmad's new media page, so the comments are considered published by Ahmad. In addition, it is different from the Printing Presses and Publications Act 1984, the Evidence Act 1950 (Amendment) 2012 has a clearer definition regarding a publication i.e. a statement or a representation, whether in writing, printed, pictorial, film, graphic, acoustic or other form displayed on the screen of a computer.

k) Penal Code (Act 574)

In addition, the results of document analysis found the Penal Code or better known as Act 574 can be applied to cyber crime offenses. Pornography issue may create a big challenge to the country. Through this research, it can be found that there are several provisions in the Penal Code to regulate the issue of pornography in new media. Section 292 in general can be applies to pornographic offenses in cyberspace. According to Rahim & Manap (2004), pornography carries the meaning of any book, pamphlet, paper, diagram, drawing, illustration or statue that is obscene or any other obscene thing in subsection (a) above describes this section can be applied to pornographic activities on the new media. Pornography materials can be possessed in several forms such as in printed form, digital form published form, magnetic or electronic form nor in the form of a diskette, pendrive, or compact disc. Now, the new media can be accessed by anyone and anywhere including children. It would be a big concern if children are also exposed as an new media user to pornography materials. In the Children Act 2001 section 2 only mean to children under the age of eighteen years. Based on the results of document analysis, there are another provision under section 377E of the Penal Code where it's offense refer to any child to commit an obscenity act. Therefore, those who incite any child to commit an obscene act on any website may also be subject to action under the above section (Rahim & Manap 2004). The penal code helps to address the problem of sexual harassment through new media. In addition to the issue of pornography, the Penal Code also provides for defamation issues. This can be seen under sections 499, 500, 501 and 502 of the Code Penalty.

l) Consumer Protection Act 1999 (Amendment) 2010

The results of document analysis show that this act protects the rights of users in the process of buying and selling, goods, services, contracts and others including online dealings as well as

protecting consumers in terms of obtaining information through advertisements aired or broadcasted. Advertising in printing media and electronic media can still be controlled by government side compared to online advertisements. Consumers are easily deceived by advertisements available in the new media for not knowing its authenticity. Adding to the situation, there is no agency that monitors it as a whole. In addition to legitimacy, ads on the new media also does not adhere to existing advertising guidelines and most of it is false and misleads users. Under the 2010 amendment, there is a provision of a new Division namely the XIA Advertising Committee and under section 84A where the minister may establish Advertising Committee to look into complaints regarding advertisements, advertised information on consumer rights and others. An existence of guidelines provided by the committee to avoid false advertisements or confusing. In these guidelines advertising is construed as any form of advertising in the form of speech, writing, sound, sketch or picture published through (i) display or publication of notices; (ii) the use of print media such as newspapers, magazines or printed materials such as catalogs, price lists, circulars, labels, cards or other documents or materials; (iii) a film, drawing or photograph; (iv) the use of electronic mediums such as radio, television or telecommunications online as well as any other means. These guidelines are very emphatic false ads and misleading users. In addition to this guide, the Protection Act Consumers (Amendment, 2010) 1999 also provides prohibition provisions on false or misleading conduct under sections 9 and 10. It can be concluded that these findings have answered fourth objective of this fourth study which is on the implementation of the law against cyber security threats. In law enforcement, agency or body of the government plays an important role in the enforcement aspect. Two major agencies that have a source of authority in enforcing the law especially on cyber security threats namely the Communications Commission and Malaysian Multimedia and the Royal Malaysian Police. The study also succeeded in identifying 12 acts or laws that can be implemented in controlling threats of cyber security such as the Communications and Multimedia Act 1998, the Crime Act Computer 1997, Electronic Commerce Act 2006, Digital Signature Act 1997, Personal Data Protection Act 2010, Sedition Act 1948, Defamation Act 1957, Act Printing Presses and Publications 1984, Copyright Act 1987, Evidence Act 1950, Penal Code as well as the Consumer Protection Act 1999. However, there are some acts required improvements such as the Communications and Multimedia Act 1998, the Criminal Act Computer 1997 and so on.

Conclusion

The element of cyber security awareness is very important among Internet users in Malaysia. This can be seen in the surge increase of cyber criminal cases reported by the press. In the conjunction of that have raised concerns among Malaysian. Satistics incident of cybersecutiy by MyCert, CyberSecurity Malaysia had display an escalating in the number of cases form start the Year 2015 with 571 006 cases to the Year of 2016 with 740 774 cases reported and more increase until now. This shown a huge responsibility in the cyber security incidents and cannot be taken lightly by Malaysian. Besides, Content Supervision and Enforcement Division of MCMC have expressed a disappointment towards Malaysian.This is because the statistic release by them showed an increase in the number of Internet cases in 2015 with a total of 2536 cases were reported and this figure increased in the Year 2016 with 2614 cases as reported to MCMC.

Government's decision to advancing in the field of ICT has created an apportunity for the criminals to commit a crime. Thus, it cannot be denied as the cases of cyber crime keeps increasing day by day. Most of the cyber crimes reported are like cyberbullying, transmit

viruses to other individuals, hacking, spread andvcreating various pornographic sites, sending phishing emails, online scams, spreading false and slanderous news and more acts that are against Malaysian law. In the context of cybercrime, various security measures were taken and introduced by the government agencies through programs such as Click Wisely, CyberSAFE and other to motivate people in creating awareness to Internet users. Unfortunately, to be concern is to what level of Internet users have the awareness towards cyber security. As the number of cyber crime cases keep increases, there are still more users who did not aware on this and neglect the security aspects when using of Internet. The more Internet users rely on the Internet, the more opportunities they are exposed to cybercriminal. Hence, the element of awareness is necessary to be enhanced in every individual in Malaysia.

Firstly, Internet users need to understand the concept of awareness clearly so that they can appreciate the importance of cyber security awareness. In order to gain self - awareness then each of the Internet users need to take note of the relevant agencies in charge of Malaysian cyber security. These agencies are responsible in providing the knowledge and advocacy of cyber security programs. In addition, Internet users need to aware on relevant regulations and laws on safety cyber. By this law may provide knowledge to Internet users in defending their rights and protect themselves from cyber threats. By right, these measures can certainly increase the level of awareness among Internet users on cybersecurity.

Moreover, not limit to Internet user only, every individual needs be more observant towards strange activities happening in Internet to themselves or friends like being a victim of cyberbullying, victims of pornography, victims of fraud and so on. This experience can help Internet users to always be careful when using of Internet. Besides that, the experience may help Internet users to take an appropriate action according to the situation as a cyber victim. Other than that, social environmental factor is also very important in raising the level of awareness of Internet users. Such factors like parental upbringing, peer influence, workplace roles, mass media's roles, and government policy need to be focused and accessed on how far these factors can help Internet users in protecting themselves against cyber threats. In addition, the implementation of cyber law is very important in curbing or reducing cybercrime. With the provisions of cyber law and stricter punishment can reduce the issue of cyber crime in Malaysia.

Contribution and Motivation of this Study

The results of this study will serve as an indicator to the government to introduce a new Cyber Security bill which is intended to combat a variety of cybercrimes. In fact, this also serve as an indicators to the government to understand the main challenge concerning to cybersecurity crime nowadays and accelerate their legislative programs particularly in respect of technology and cyber related laws, whether to accommodate digital activities within existing legislation or to reflect new realities with new legislation.

References

Aarssen, L. W., & Crimi, L. (2016). Legacy, Leisure and the 'Work Hard–Play Hard'Hypothesis. *The Open Psychology Journal*, *9*(1).

Fleming-Milici, F., & Harris, J. L. (2020). Adolescents' engagement with unhealthy food and beverage brands on social media. *Appetite*, *146*, 104501.

Jerde, R. D. (2017). *Follow the Silk Road: How Internet affordances influence and transform crime and law enforcement*. Naval Postgraduate School.

Jiang, Q., Huang, X., & Tao, R. (2018). Examining factors influencing internet addiction and adolescent risk behaviors among excessive internet users. *Health communication*, *33*(12), 1434-1444.

Markom, R., Zainol, Z. A., & Fuad, N. A. (2019). Literasi perundangan media baharu dalam kalangan belia. *Jurnal Komunikasi; Malaysian Journal of Communication*, *35*(3), 372-389.

Adnan, M. (2013), in addition to social environment factors, there are several other factors that drive cybercriminals to commit such offenses.

Rahim, A. A., & Manap, N. A. (2004). Perspektif Terkait Kejahatan Komputer Hukum Malaysia.