Society 5.0

Integrating Digital World and Real World to Resolve Challenges in Business and Society

Society 5.0 2021

Proceedings of the

First International Conference on Society 5.0

Virtual Forum 22nd to 24th June 2021

Editors: Aurona Gerber & Knut Hinkelmann

Copyright Notice

The Society 5.0 2021 organising committee is not responsible for errors or omissions from individual papers contained in these proceedings. Technical electronic anomalies are possible and unavoidable during the compilation process. The publisher is not responsible for the accuracy and validity of information contained in these papers, nor is it responsible for the final use to which this book may be used.

The Society 5.0 2021 Proceedings Editors attest as follows: All conference paper submissions that appear in these proceedings have been through a blind peer review process prior to acceptance into the final conference programme.

Editors:
Aurona Gerber, Department of Informatics, University of Pretoria, and
Knut Hinkelmann, FHNW University of Applied Sciences and Arts Northwestern Switzerland

Published by the Society 5.0 editors

Organization

The annual conference series is jointly organized by the Universidad EAFIT (Colombia), the University of Pretoria (South Africa), University of Camerino (Italy), the Business School of the Shenzhen Technology University (China), the Universiti Malaysia Kelantan (Malaysia), Putra Business School (Malaysia) and the FHNW University of Applied Sciences and Arts Northwestern Switzerland.

Steering Committee

Patrick Renz (chair)	FHNW University of Applied Sciences and Arts Northwestern Switzerland
Ahmad Shaharudin Abdul Latiff	Putra Business School, Malaysia
Marc Aeschbacher	FHNW University of Applied Sciences and Arts Northwestern Switzerland
Sara Aguilar-Barrientos	Universidad EAFIT, Colombia
Roselina Ahmad Saufi	Universiti Malaysia Kelantan, Malaysia
Carolina Ardila-López	Universidad EAFIT, Colombia
Noorshella Che Nawi	Universiti Malaysia Kelantan, Malaysia
Flavio Corradini	University of Camerino, Italy
Zhuoqi Ding	Shenzhen Technology University, SZTU Business School, China
Wan Fadzilah Wan Yusoff	Putra Business School, Malaysia
Aurona Gerber	University of Pretoria, South Africa
Knut Hinkelmannn	FHNW University of Applied Sciences and Arts Northwestern Switzerland
Stephan Jüngling	FHNW University of Applied Sciences and Arts Northwestern Switzerland
Gordana Kierans	Shenzhen Technology University, SZTU Business School, China
Hanlie Smuts	University of Pretoria, South Africa
Arie Hans Verkuil	FHNW University of Applied Sciences and Arts Northwestern Switzerland

Program Committee Chairs

Technical Chairs

Aurona Gerber	University of Pretoria, South Africa & Centre of AI Research (CAIR), South Africa
Knut Hinkelmann	FHNW University of Applied Sciences and Arts Northwestern Switzerland

Organising Committee

Marc Aeschbacher	FHNW University of Applied Sciences and Arts Northwestern Switzerland
Devid Montecchiari	FHNW University of Applied Sciences and Arts Northwestern Switzerland

Awareness on Financial Cybercrimes among Youth: Experience, Exposure and Effect

Farah Hanan Muhamad[1[0000-0001-6882-846X]], Mohd Zulkifli Muhammad[1[0000-0001-9700-454X]], Siti Fariha Muhamad[1[0000-00020-3119-1861]] and Nur Syafiqah Binti A. Samad[1[0000-0002-0139-9386]]

[1]University of Malaysia Kelantan, Jalan Pengkalan Chepa, 16100 Kota Bharu, Kelantan
farahhanan@umk.edu.my

Abstract. After converging into information technology in the last three decades, Malaysia has transformed into a regional Information Communication Technology (ICT) hub. Despite its bundle benefits to the user, the package comes together with related risk exposures and has gradually evolved since then. The purpose of this paper is to find out whether the constructs related to the awareness of youth in terms of experience, exposure, effects of financial cybercrime. This study adopts a quantitative approach by using Pearson's correlation analysis to explain the data which has been collected through a structured questionnaire. A total of 242 respondents have participated in this study via a convenience sampling method. The finding revealed that youth are reasonably aware of the financial cybercrimes based on the constructs used in this study. Although this research has been carefully prepared and achieved its goals, it is still known that researchers are limited and deficient. Firstly, the scope of analysis will likely be limited by the scarcity of evidence or reliable data. Most journals have found that there is a dearth of information on e-banking in Malaysia compared to other developing countries.

Keywords: *cybercrime, youth, financial, awareness*

1 Introduction

Financial technology nowadays has become one of the strength pillars to the growth of a nation. After converging into information technology in the last three decades, Malaysia has transformed into a regional ICT hub. As stated in Shared Prosperity Vision 2030, one of the biggest challenges refrained the nation from moving forward is due to the lack of participation among industrials in digital economy. Until recently, the outbreak of pandemic has caused stir to the global economic well-being and thus increased the usage of virtual transaction among users. The finance analyst, Jonathan Curtis, sees the boom effect of technological sector and makes his statement, 'the big opportunity in this space is digital transformation' (The Edge Markets, 2020).

Hitherto, the banking activities is in the traditional form of transaction such as cash payments, cheques, or bank drafts. Moving forward this trend has paved a way to a modern system of payment in the form of swiping of debit cards or credit cards. The adoption of financial technology is perceived as a cost-effective strategy and recognized for its privilege to bring greater efficiency and productivity. Many financial and non-financial institutions invest in technological invention to create an added value to the company and remain competitive in the years ahead.

Though the benefits of technology are undeniably robust, the weaknesses are just at par (Agrawal S., 2016). Technological advancement leads to digital invention of many opportunities to the economic activities. Despites its growing demand in technological sector, the financial cybercrimes also go on strike and show an increase trend since Movement Restricted Order (MCO). This is proven by the fact that the number of cybercrime attack has increased for the same period as MCO from March 18 to April 7 by 82.5% from 417 cases in year 2018, 459 cases in year 2019 and recently the cases has jumped to 838 (TheStar, 2020). As of this year, the total cybercrimes cases in April alone is 1488 and attain the highest fraud case (MyCert, 2020). While the banking sector was able to reach more customers with the emergence of advanced technology, it also increased the risk for customers, who often have doubts and insecurity regarding these services.

There are several types of cyber-criminal activity which has been recognized as serious crime in Malaysia such as cyber harassment, intrusion attempt, intrusion, vulnerabilities report, denial of service, fraud, malicious codes, spam, and content related. The laws regulated purposely for cybercrime are as follows; Computer Crime Act 1997, Communications and Multimedia Act 1998, Malaysian Communications and Multimedia Commission Act 1998, Digital Signature Act 1997, Copyright Act (Amendment) 1997, Telemedicine Act 1997, Optical Disc Act 2000 and Electronic Transactions Act (2006). As part of initiative to counter the rising cybercrime cases, it is important to educate the young generations on awareness about cyber law and regulations (Chanuvai Narahari & Shah, 2016).

At present, cybercrime is a growing threat and is most prevalent in the digital world since individuals and groups rely more on information technology to finish off the dealings with faster transaction such as online banking over automated teller machines (ATM). The rapid use of the internet and other technology in the banking sector has increased the likelihood of cyber threat across the world such as scammers, phishing, hacking etc. Hence, it is necessary for researchers to investigate and review the cybercrime scenario in a country because it is new in Malaysia. The user of financial technology has no age limit, thus vast number of people will find this study helpful for them especially related industry such as technological sector to come up with defensive blocking system due to increasing cybercrime cases in financial sector, youth who actively connected to the internet, government agencies and public institutions. The purpose of this paper is to find out on the constructs related to the youth awareness on financial cybercrimes in terms of, experience, exposure, and effects.

2 Literature Review

2.1 Financial cybercrimes

Though technology makes thing easier, effective, and efficient, the misuse of technology by some irresponsible parties has led to a gruesome situation. Besides, the age of a person is not a pre-requisite from being a victim of this growing concern issue. Together in this, Amro (2017) said, "with an increasing number of individuals staying in touch using mobile devices, cyber threats are becoming increasingly prevalent among all age groups." It is well explained by Albert (2018), who emphasized the responsibility of young generation to protect older adults from being a victim of cybercrime as nowadays they are the most vulnerable target aimed by cybercriminals. Therefore, the youth should be playing the role and well-adapted with knowledge to exercise the duty.

As described by Agrawal S. (2016), internet banking users should stay cautious from financial cybercrime and be able to avert fraud and take a necessary step for security mechanisms so that they do not become victims of cybercrimes. In another part of the world, cybercrime cases in Africa also depicting a rising figure as evidenced by the country's annual losses to cybercrimes were estimated for Nigeria at $649 million, and Kenya at $210 million. In pursuance to this issue, Kshetri (2019) offered his thought in cybersecurity legislation and enforcement measures in the continent to further counter the rising cases.

This study adopts Routine Activity Theory (RAT) and Lifestyle Exposure Theory (LET) in the study as it ideally clarified cyber criminology and its consequences to the young and youth age. According to the Leukfeldt & Yar (2016) and Williams et al. (2019), the former theory is explaining victimization of cybercrime and its connection to the business cybercrime. On the other hand, the latter suggests that different lifestyle may expose people to different circumstances and it ends up getting into crime-prone situations which lead to a higher risk of victimization (Elly, n.d.). Rendering to Mugari, Gona, Maunga, & Chiyambiro, (2016), several types of cybercrimes such as hacking, phishing, identity theft and malware are amongst the threat of financial sectors in Zimbabwe. As conformed by Chevers (2019), who perceive the usage and frequency of using electronic banking are influenced by the first three crimes mentioned earlier as negative impact to adoption of electronic banking due to its continual escalation in financial cybercrime.

2.2 The experience of financial cybercrimes

As demand for access to online banking continues to increase and many customers rely on technology at fingertip for managing their finances, banks and other financial service companies would ensure that these transactions are convenient to perform. In a study conducted by Virtanen (2017), he summarized that, "experiences with hacked accounts

or cyberattacks also intensifies the fear of those with low confidence more than those with a higher amount of confidence." Therefore, he stands on his argument that social and physical vulnerabilities as well as victimization have direct and indirect effects on fear of cybercrime.

It is fairly important to be able to study on the likelihood behavior to become a victim of cybercrime. Van de Weijer & Leukfeldt (2017) agreed that only individuals with higher scores on openness to experience have higher odds of becoming a victim of cyber-enabled crimes.

$\mathbf{H_0}$: Victim experience has no significant correlation to the youth awareness on financial cybercrimes

$\mathbf{H_1}$: Victim experience has significant correlation to the youth awareness on financial cybercrime

2.3 The exposure of financial cybercrimes

The existence of cybercrimes has generated element of risk exposure that give effects to the personal harm and organizational harm. According to Verma, Hussain & Kushwah (2012), the risk exposure includes several items which are financial losses, regulatory issues, data breach liabilities, damage to brand and reputation, and loss of client and public confidence. Exposure is perceived as one of the major components to be victimised in cybercrimes (Phillips, 2015).

$\mathbf{H_0}$: The risk exposure of using electronic banking has no significant correlation to the youth awareness of financial cybercrime

$\mathbf{H_2}$: The risk exposure of using electronic banking has significant correlation to the youth awareness of financial cybercrime

2.4 The effects of financial cybercrimes

The person who involve in making the cybercriminals have developed advanced technique that increase the types of cybercrimes such as spying the business activities and access important business information which indirect impacts the bank's finances. This is supported by who has similar views on the impact of cybercrimes towards financial activities. The effects of a single, successful cyber-attack can have far-reaching implications, including financial losses, theft of intellectual property, and loss of consumer confidence and trust.

Becoming the victim of cybercrimes can have a long-lasting effect in an individual's life. In a study investigated by Kaakinen, Keipi, Räsänen, & Oksanen (2018), the result indicated as per se, "analogously to crime victimization in the offline context, cybercrime is a harmful experience whose negative effects mainly concern those users who have weak social ties offline to aid in coping with such stressors."

$\mathbf{H_0}$: Acknowledge the effect of using electronic banking has no significant correlation to the youth awareness on financial cybercrimes

$\mathbf{H_3}$: Acknowledge the effect of using electronic banking has significant correlation to the youth awareness on financial cybercrimes

3 Method

3.1 Research Design

This study is conducted in a quantitative manner. The aim of the study was to determine whether fourth-year students in the Faculty of Entrepreneurship and Business (FKP) at University Malaysia Kelantan's City Campus were aware of cybercrimes involving the e-banking system. In this report, descriptive and correlation analysis were used. As interpreted, the intention of the analysis was to investigate the relationship between the motives and the independent variables.

3.2 Unit of Analysis

The unit of analysis of this research will be the fourth-year students in Faculty of Entrepreneurship and Business at University Malaysia Kelantan. The respondents involved are the student selected courses, such as Logistics, Islamic Banking and Finance, Commerce and Retail, who are most likely using e-banking system.

3.3 Quantitative Research

A sample size can be defined as a subset of population. According to Roscoe (1975), sample size larger than 30 and less than 500 are appropriate for most research. By studying the samples, (Sekaran, 2010) has verbalized that the researcher should be able to meet the interest of the population. Since the total number of elements in the population frame cannot be ascertained due to unavailability of data, a precise number of samples cannot be drawn to represent the population.

Table 1: Krejcie and Morgan Sample Size Table

Table for Determining Sample Size of a Known Population

N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	346
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	354
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	191	1200	291	6000	361
45	40	170	118	400	196	1300	297	7000	364
50	44	180	123	420	201	1400	302	8000	367
55	48	190	127	440	205	1500	306	9000	368
60	52	200	132	460	210	1600	310	10000	370
65	56	210	136	480	214	1700	313	15000	375
70	59	220	140	500	217	1800	317	20000	377
75	63	230	144	550	226	1900	320	30000	379
80	66	240	148	600	234	2000	322	40000	380
85	70	250	152	650	242	2200	327	50000	381
90	73	260	155	700	248	2400	331	75000	382
95	76	270	159	750	254	2600	335	1000000	384

Note: N is Population Size; S is Sample Size *Source: Krejcie & Morgan, 1970*

Based on Krejcie and Morgan (1970) table above, researcher will select 242 students as a sample from the total of 681 students. The respondents will answer the questionnaire itemized on the awareness of cybercrimes involved in the e-banking system among fourth year students in Faculty of Entrepreneurship and Business at University Malaysia Kelantan.

3.4 Development of Questionnaire

There are three sections in this questionnaire. First is section A which will discuss about the background of the respondents. Then, section B contains the question about the dependent variables (generally). Lastly, Section C, D and E explains the questionnaire item on each independent variable; the experience of cybercrimes in e-banking, exposure of cybercrimes in e-banking and effect of cybercrimes in e-banking. All the items to be included in the questionnaire were set on three points of scale, which is interpreted such as:

3.5 Data Analysis Procedure

Research data are collected frequently either by qualitative or quantitative methods (Hawe, Degeling, Hall, 1990). Questionnaires, surveys, and other quantitative approaches are used to collect data. According to Babbie (2010), numerical data and generalization across groups of people are collected and explained in a quantitative research. According to Avasarikar (2007), primary data is a term for data collected for a specific purpose, such as the preferences of researchers' requirements for any research problems.

The researcher uses a questionnaire method to gather all information in this research. Usually, questionnaire approaches are less costly and easier to perform. They are also relatively easy to implement because they are structured and free of many forms of error. It is usually intended for large amounts of quantitative data collection. A set of questionnaires will be distributed to the students. Respondents will be asked to answer all the questions in a timely manner. Respondents are also aided in clarifying the questions.

The data collected from the survey questionnaire will be calculated and evaluated with software version 23.0 of the Statistical Social Science Package (SPSS). The analysis of the data will be construed as two stages. The first phase of the data analysis includes the conduct of an analysis of the data to examine the data before any statistical procedures are adopted. The raw results, average values and relative values are calculated for each respondent. These data are the basis for further analysis.

3.6 Validity and Reliability

The concepts of validity and reliability were also used in this study. It is to understand how to minimize the possibility of errors and tendencies by increasing the data's reliability and validity. Conferring to Messick (1989), validity evolved into a complicated

concept. It is more closely related to the conclusion based on the assessment results. That is more focused on the outcome of the speculation that makes it implied. This evaluating consideration must be accurate and declare the truth. The assessment or evaluation should not be valid; only the assumption about this evaluation should be valid. Reliability coefficient assesses the consistency of the entire scale with Cronbach's Alpha being the most widely used measure (Nunnally, 1979). On other hand, the validity is the extent to which an instrument measures it is supposed to measure (Wiersma, 2000).

4 Results

After collecting the data from the respondents, the results of the research are started to analyze. To do so, the results collected from the distributed questionnaires were entered into the Statistical Package for Social Science (SPSS) version 23.0. Section A, which is the demographic part is first to be analyzed according to the questionnaire, that consist of gender, age, race, course and where do they access internet the most. Then, section B, C, D and E where it includes the Likert Scale measurement for every question asked to assess youths' understanding towards financial cybercrime.

4.1 Cronbach's Alpha

As shown in the Table 1, Cronbach's alpha is used to measure internal consistency or reliability of the items. To understand whether the questions in this questionnaire all are reliably measured the same latent variable, a Cronbach's alpha was measured on a sample size of 30 respondents.

Table 2: Cronbach's Alpha Coefficient Range

No	Coefficient of Cronbach's Alpha	Reliability Level
1	More than 0.90	Excellent
2	0.80-0.89	Good
3	0.70-0.79	Acceptable
4	0.60-0.69	Questionable
5	0.50-0.59	Poor
6	Less than 0.59	Unacceptable

The overall result of Cronbach's alpha is **0.974**, which indicates too high as it may have similarity and overlapping of the items since the suggested alpha value should be in within 0.65 to 0.95 (Piaw, 2012).

Table 3: Reliability Statistics

Cronbach's Alpha	N of Items
.974	20

4.2 Demographic Profile

Demographic profile is used to describe the phenomenon of a variable. In this study, categorical variables such as nominal and dichotomous were used to further assess the background of the sample such as gender, age, race, and internet accessibility.

Table 4: Demographic Analysis

No.	Profile	Description	Frequency	Percentage (%)
1.	Gender	Male	81	33.5
		Female	161	66.5
2.	Age	16-20	124	51.2
		21-25	103	42.6
		26-30	15	6.2
3.	Race	Malay	185	76.4
		Chinese	34	14.0
		Indian	21	8.7
		Others	2	0.8
4.	Internet sources	Home	69	28.5
		College	165	68.2
		Cyber café	1	0.4
		Others	7	2.9

Table 3 demonstrated a summarization of frequency analysis for 242 respondents who had participated in this survey. Firstly, most of the respondents are female which constitutes 66.5% (161 respondents), while male consists of 33.5 % (81 respondents). Meanwhile, majority of them aged from 16 to 20 years old with 51.2 % (124 respondents), followed by those who aged 21 to 25 years old with 42.6% (103 respondents) and the rest is 6.2% (15 respondents).

Of the total respondents, 76.4 % (185 respondent) answered by Malay respondents compared to Chinese with 14 % (34 respondents) and 8.7% (21 respondents) among

Indian. The remaining of 0.8 % (2 respondents) were from other races. This can be concluded that Malay was most of the youth population in the community.

According to the respondents, many of them get access to the internet from college approximately 68.2 % (165 respondents), then home is the second place where they highly accessed the internet constitutes of 28.5 % (69 respondents), while 2.9 % of respondents prefer other places to access (7 respondents and lastly access at cyber cafe with 0.4 % (1 respondents). Therefore, those who are staying in the campus are the most users of internet.

4.3 Descriptive Analysis

Descriptive analysis is a method used by researchers to identify the number in statistical interpretations and sum of the value. This study relies on mean and standard deviations to explain the measure of dispersion.

Table 5: Result of Descriptive Statistic

Variables	Mean	Std. Deviation
Influenced factors		
Experience (IV1)	3.11	0.462
Exposure (IV2)	3.34	0.481
Effect (IV3)	3.29	0.503
Awareness of cybercrimes	3.23	0.491

The table above shows, the summary of descriptive statistics of the influenced factors in this study. From the results, the highest mean belongs to exposure which obtain 3.34 while the lowest mean is 3.11 for experience factor. Meanwhile the effect factor shows the strongest dispersion of 0.503 and the lowest is experience at 0.462. The average dispersion measured by these analyses are 3.23 and 0.491, respectively.

4.4 Pearson Correlation Analysis

As part of inferential analysis, its purpose is seen important to describe the characteristics of the research subjects by identifying the relationship of the variables. SPSS is used in this part to analyze if there exist a strong strength of association between the two variables involved. Along this line, the dependent variable of the research is youth awareness towards financial cybercrimes while the independent variable is experience, exposures, and effects.

Table 6: Rule of Thumb for Interpreting the Size of a Correlation Coefficient

Size of Correlation	Interpretation
.90 to 1.00 (−.90 to −1.00)	Very high positive (negative) correlation
.70 to .90 (−.70 to −.90)	High positive (negative) correlation
.50 to .70 (−.50 to −.70)	Moderate positive (negative) correlation
.30 to .50 (−.30 to −.50)	Low positive (negative) correlation
.00 to .30 (.00 to −.30)	negligible correlation

Table 3 portrays the rule of thumb for interpreting the size of a correlation coefficient as it describes the strength of the relationship among the variables. The connection coefficient or allude as r. If value of r is +1.0, there is an impeccable positive relationship and if the estimation of r is -0.1, it immaculate the negative relationship of the factors. When the point estimation is r=0, it is demonstrated as no relationship between the factors of the research.

		Awareness
Experience	Pearson Correlation	.651**
	Sig. (2-tailed)	.000
	N	242
Exposure	Pearson Correlation	.589**
	Sig. (2-tailed)	.000
	N	242
Effect	Pearson Correlation	.503**
	Sig. (2-tailed)	.000
	N	242

The value of correlation coefficient for awareness of youth and experience is 0.651 which indicates a moderate relationship. The p-value is significant at 0.000 which is lower than 0.01. From the results attained, it can be concluded that experience has positive strength of relationship to the awareness of financial cybercrime among youth. Therefore, this be can concluded that $\mathbf{H_1}$ is accepted.

Meanwhile, the value of correlation coefficient for awareness of youth towards exposure of cybercrime is 0.589 and thus defines moderate relationship for both of variables. The p-value is 0.000 which is lower than 0.01. As stated in the table above, there

exists a positive strength between exposure and awareness of financial cybercrimes which explains. Thus, **H_2** is accepted.

The above table specifies on the value of correlation coefficient between awareness of youth and effects of cybercrime is 0.503 which implies moderate relationship. The p-value is significant at 0.000 since it is lower than 0.01. Again, **H_3** is accepted.

The questionnaires were first analyzed by using Cronbach Alpha. Back to the main purpose of this study is to test the strength of relationship between experiences, exposures and effects towards youth awareness in virtual transaction. From the result, the relationship strength of all independent variable towards the dependent variable is moderately correlated with r = 0.651 (experiences), r = 0.589 (exposures) and r = 0.503 (effects) which is significant at the 0.01 level (2-tailed). It seems to suggest that all the independent variable are the factors that represent the youth awareness towards financial cybercrimes. To sum up, all the hypotheses are significant and accepted. These hypotheses have significant values of 0.000 which are less than 0.05.

5 Conclusion

This chapter will discuss and review the result and supported by the previous study. A total of 242 questionnaires were distributed to University Malaysia Kelantan students (UMK). Initially, a reliability test was used to analyze the questionnaires. The demographic profile was then examined by using frequency analysis such as gender, age, race, course, and internet sources.

The population of students has been evaluated to address the phenomenon at university level in the matter of financial cybercrimes. The demographic profile shows that 33.5% of those interviewed come from men and 66.5% from women. Furthermore, 124 people (51.2%) are between 21 and 22 years of age and less than 25 years of age and above are respondents. 185 (76.4 percent) respondents reported that they were Malay. Each course excludes 24.4% retail course while others remain at 25.2% per course. In addition, most of them have internet connectivity in the university.

In this research, the hypothesis is to test the relationship between experience, exposure, and effect of using electronic banking towards awareness in financial cybercrimes. The relationships between all independent variables and dependent variable are correlated by the hypothesis, which are important at the 0.01 level, to r = 0.650 (experiences), to r = 0.589 (exposures) and to r = 0.503 (effects). This makes it clear that all the factors are associated to the awareness in cybercrimes. All hypotheses are substantial and accepted in summary. To conclude, the cybersecurity is becoming an intense headline nowadays since it is in high demand due to increasing figure of cybercrime cases. The drive towards Fourth Industrialization Revolution (IR 4.0) will come together with risk of cyberattacks. Thus, the call for adopting a common language and framework around cybersecurity should be exercised immediately before losing more to it.

Furthermore, strong cybercrime governance and legislation and policies with specific emphasis on tackling electronic channel-based fraud. Organization require a comprehensive enterprise-wide approach to cybercrime management that supports broader organizational compliance and risk management. The path to this approach includes an information technology (IT) infrastructure that enables enterprise-wide, real time, and cross-channel monitoring and management capabilities. Bank institutions should work towards developing digital forensic auditors.

Although this research has been carefully prepared and achieved its goals, it is still known that researchers are limited and deficient. Firstly, the scope of analysis will likely be limited by scarcity of evidence or reliable data. Most journals have found that there is a dearth of information on e-banking in Malaysia compared to other developing countries. Moreover, the studies affect only 242 students at the Malaysia Kelantan University, the City Campus as a sample and do not represent the entire population at Kelantan University. A wide range of research is therefore recommended and preferable. The limitation issue that occurs in this research should be addressed in future research. If the scope of the study is wider, the results of the research are better and the community such as students and staff can benefit significantly. Conversely, the study should be conducted using a qualitative approach, in which the researcher will interview the respondent to obtain knowledge from their own perspective about their own experience, how aware they are of cybercrime, and what impact cybercrime has had on them.

References

1. Agrawal, S. 2016 (May). Cybercrimes in Banking Sectors. *Volume 3, "ISSN 2455-2488"*

2. Verma, M., Hussain, S.A. & Kuswah, S.S. (2012). Cyber Law: Approach To Prevent Cyber Crime. IJRREST: International Journal of Research Review in Engineering Science and Technology, 1(3), 123 – 129.

3. Albert, M. (2018). *A New and Growing Problem for Older Adults*. 2017–2019.

4. Amro, S. Al. (2017). Cybercrime in Saudi Arabia: fact or fiction? *International Journal of Computer Science Issues*, *14*(2), 36–42. https://doi.org/10.20943/01201702.3642

5. Chanuvai Narahari, A., & Shah, V. (2016). Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India). *Ijariie*, *6*, 2395–4396. http://ijariie.com/AdminUploadPdf/Cyber_Crime_and_Security_–_A_Study_on_Awareness_among_Young_Netizens_of_Anand__Gujarat_State__India__ijariie3502.pdf

6. Chevers, D. A. (2019). *The impact of cybercrime on e-banking : A proposed model*. 10.

7. Elly, T. (n.d.). *Cybercrime – Factors Influencing the Adoption and Use of Electronic Financial Services in Tanzania Violete Rwezaura and Introduction The information revolutions coupled with strategic use of the internet , has exposed a number of relatively open societies*. 1–22.

8. Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 129–137. https://doi.org/10.1089/cyber.2016.0728

9. Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

10. Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

11. Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe. *Mediterranean Journal of Social Sciences*, *7*(3), 135–143. https://doi.org/10.5901/mjss.2016.v7n3s1p135

12. MyCert. (2020). *Reported Incidents Based on General Incident Classification Statistics 2020*. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=f88181d6-9839-4828-a612-1d27c820e1af

13. New Straits Times. (2019). "Youth" now defined as those between 15 and 30. *New Straits Times Press*. https://www.nst.com.my/news/nation/2019/07/501288/youth-now-defined-those-between-15-and-30

14. Phillips, E. (2015). Empirical Assessment of Lifestyle-Routine Activity and Social Learning Theory on Cybercrime Offending. *Department of Criminal Justice*. http://vc.bridgew.edu/cgi/viewcontent.cgi?article=1024&context=theses

15. Piaw, C. Y. (2012). Mastering research methods. In *Journal* (Vol. 2, Issue 2012).

16. Star, T. (2020). *Cybersecurity cases rise by 82.5%*. https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825

17. The Edge Markets. (2020). Tech sector to see "powerful acceleration" on earnings growth post Covid-19. *The Edge Communications Sdn. Bhd.* https://www.theedgemarkets.com/article/tech-sector-see-powerful-acceleration-earnings-

growth-post-covid19-—-franklin-templeton

18. Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

19. Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law*, *24*(3), 323–338. https://doi.org/10.1080/13218719.2017.1315785

20. Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior*, *40*(9), 1119–1131. https://doi.org/10.1080/01639625.2018.1461786

21. Hawe, P., Degeling, D., & Hall, J. (1990). Evaluating Health Promotion: A Health Workers's Guide. Sydney, MacLennan & Petty.