Print ISSN: 2233-4165 / Online ISSN 2233-5382
JIDB website: http://www.jidb.or.kr
doi:http://dx.doi.org/10.13106/jidb.2021.vol12.no12.1

The Relationship Between Financial Literacy and Public Awareness on Combating the Threat of Cybercrime in Malaysia

Mohd Yaziz Bin Mohd ISA[1], Wan Nora Binti Wan IBRAHIM[2], Zulkifflee MOHAMED[3]

Received: October 21, 2021. Revised: December 02, 2021. Accepted: December 05, 2021.

Abstract

Purpose: Cyber criminals have affected various markets and the banking system has encountered various kinds of cyberattacks. The purpose of this study is to analyze cybercrime that is an emerging threat and investigate the significant contribution of financial literacy and public awareness on cybercrimes. To understand the security issues and the need for corrective steps, the techniques and strategies used by cyber fraudsters in obtaining unauthorized access and use the financial information for purpose of fraud need to be understood. **Research design, data and methodology:** A sample of 123 banks employees from 12 commercial banks in Malaysia was surveyed. This study differs from previous studies as it surveyed the employees' awareness, and this approach fills in the gap in existing literature. **Results:** The financial literacy and public awareness have positive impact on organizational performance effectiveness to combat threat of cybercrime. Some recommendations are also proposed from research findings, for banking industry and government regulations. **Conclusion:** The present study focuses on banking sector so its findings cannot be generalized to other sectors. Linking these topics has created a new study in combating threat of cybercrimes generally, and specifically in Malaysia. The present study enhances the understanding of customers' role to combat the impact of cybercrimes on performances of banking industry.

Keywords : Cybercrime, Banking Sector, Financial Literacy, Public Awareness

JEL Classification Code: G15, G20, G29, G40

1. Introduction[1,2]

In modern computer technologies and data networks, people seldom are to rob money from the vault because there are lots more of money that exists in cyber space. Banks adapt to modern trends of doing business through electronic medium and at the same time to protect themselves from cybercrimes. A cybercrime is the illegal and criminal activities that utilize the technology which involve a computer and network from all places in the world. It is on the rise with cyber-criminals taking advantage of advancement in new technology. It is used either as a medium of the activities or a target. Anyone with a working computer and access to the network or internet can be exposed to cybercriminals. It can affect any online users in the office, banks, business operators,

[1] First Author. Assoc Prof Dr., Graduate School of Business, Universiti Tun Abdul Razak, Malaysia. Email: mohd_yaziz@unirazak.edu.my

[2] Second Author. Postgraduate Student, Graduate School of Business, Universiti Tun Abdul Razak, Malaysia, Email: w.nora197@ur.unirazak.edu.my

[3] Third Author. Professor, School of Accounting & Taxation, Universiti Tun Abdul Razak, Malaysia, Email: zulkifflee@unirazak.edu.my

government departments, school, universities as well as individuals.

There are various types of cybercrimes. Some of the more common types of cybercrime are DDOS Attacks, Botnet, and Identity Theft. Others are Web browser fraud, identity theft (where personal data is hacked and used), theft of monetary or card financial data, theft and selling of company data, cyber extortion (demanding money to avoid a threatened attack) and cyber criminals are some other forms of cybercrimes (that are types of cyber extortion). Some of the most dangerous cyber hazards and strongest forms of malware attacks are Ransomware, Trojan Horse Programs, Computer Viruses and Worms, File Infections, System Infections, Logic Bombs, Worms and Droppers (Gupta, 2012).

Generally, commercial banks aggressively promote the development of e-banking (digital banking) to deliver fast and efficient banking services to all customers. The transactions will use a medium of digital channels with minimal brick-and-mortar presence. However, cybercrime remains rampant in the banking sector with cyber-criminals taking advantage of new digital technologies.

Computer criminals always seek unpermitted access to confidential data or financial falsified activity information. The implications of the rising cybercrime wave can make any country biggest commercial decline, leading to financial damages, theft of trade secrets, negative impacts on financial institutions' goodwill and economic development. The loss of customer trust in the digital banking system is indirectly influenced by fraud and bribery across in both developed and developing nations.
This study will focus on the financial literacy and public awareness of cybercrime methodology. The objective is not only a way to tackle cybercrime but also to establish preventive methods by defining suitable methods which fraud is performed and committed. By adopting cybercrime mitigation guidelines, successful control mechanisms must be enforced not only to support banking sectors from losses of revenue and assets, but also to enhance the efficiency of commercial banks and the overall credibility in the business setting.

To understand the security issues and the need for corrective steps, there is a need to understand the techniques and strategies used by cyber fraudsters in obtaining unauthorized access and use the financial information for purpose of fraud. Identity theft is one of the common techniques used by computer hackers when dealing with online businesses, in particular online banking medium, where fraudulent use of the identity of another person or third party, such as with the identities bank card, name, date of birth for criminal actions. Any information collected by cyber criminals via identity theft can be used for whatsoever purpose such as applying for loans, opening of account, credit card application. Phishing is a technique used by cybercrime and fraudsters in making victims known to them. There are several techniques used by phishing cyber fraudsters, but the most effective strategies are to send phishing emails to online banking clients.

Vishing or malware using voice-based phishing is a way of using VOIP, Voice over IP, computer scam artist technology to access the details of banking customers and financial information from a fake call center. The e-mail system is used to achieve this purpose by scammers who ask online banking customers to verify their bank information as well as other information as a protection routine on the phone, believing that electronic services are provided by a legitimate company/organization. Malware is the most significant vulnerability available to cyber criminals to gain unauthorized access to systems to steal their monetary as well as other confidential data malware (Viruses, Viruses, Trojans and other threats). The rapid growth of mobile devices such as cars and tablets are contributing to the development of more malicious malware. Over the past few years, malware applications (Worms, Trojan, Malware and other threats) have been used by malware as the most critical obstacle for cybercrime to gain unauthorized access to systems and steal their financial information as well as other confidential material. The rapid growth of mobile items, for examples smartphones and tablets, personal computers, contributes to high potential of malicious malware apps. In recent years, computer fraudsters have been using malware programs to commit frauds against online customers in the business sector and online banking with the intention of extracting large amounts of money.

Cybercrime is the illegal activity of grabbing monetary profit through profit-driven illegal activities in the finance and banking sectors, including identity theft, financial fraud, e-mails, and internet fraud, and attempts to steal data from consumers, relation to finance account, internet banking, credit card or other bank account details. The main financial sector-related cybercrimes include DOS virus attacks, unauthorized entry, hacking and website defacement, according to Gordon and Loeb (2003).

Online banking customers' behavior of over 100 users of online banking have been assessed to effect on users of cyberattacks according to Ali, Ali, Surendran, and Thomas (2017). The study surveyed a total of 110 banking customers and three high schools, and the data was collected from banking customers aged 18 years and above.

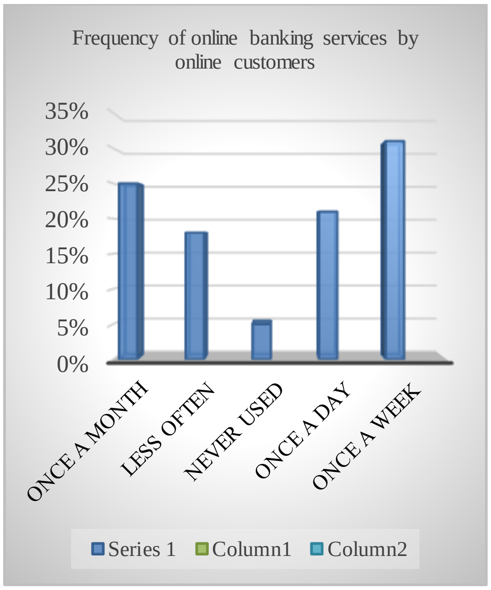

Diagram 1: Frequency Measurement

Diagram 1 above reveals only 21 per cent of users of the online banking facility each day and 31 per cent use online banking facility once a week. The study indicates that participants do online banking with the exceptions of 5%. 25% of respondents indicated that they use the online banking facility. Once in a month, 18 per cent reported that they were using these programs less regularly.

Next, diagram 2 shows the level of knowledge among respondents about online banking facility and potential of cyber-criminal. As shown in the diagram 37% of respondents were aware of computer hacking, 6 percent were aware of phishing, while another 6 percent reported that they were aware of hacking (phishing over VOIP). Out of 110 respondents, 13 per cent reported their perception of the robbery and 5 per cent confirmed their knowledge of the theft.

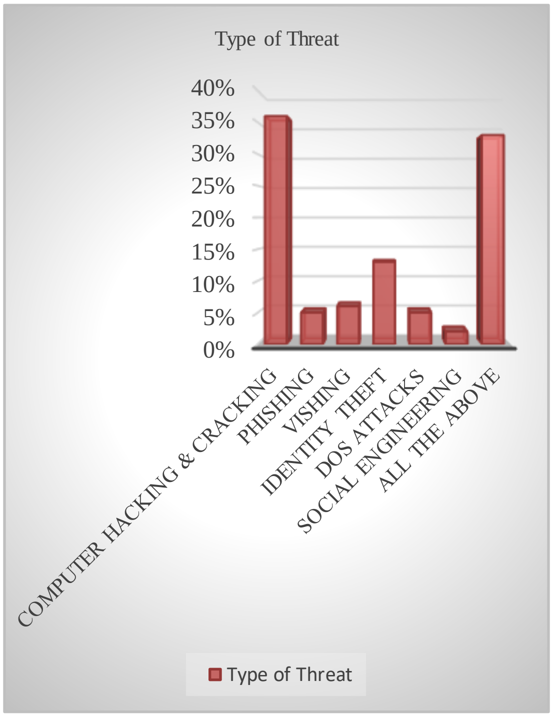

Diagram 2: Awareness Measurement

In Malaysia, in 2020, statistics provided by the Malaysian Computer Emergency Response Team (MyCERT) recorded 8,366 cases of cybercrime incidents from January to September 2020.

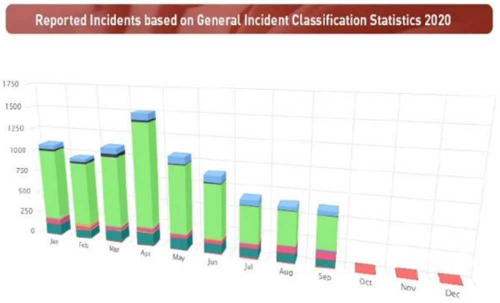

Figure 1: Incidents of Cyber Fraud

The above Figure 1 reveals a total a total of 5,697 incidents of cyber fraud were also reported to Cybersecurity Malaysia for the period from January to August in 2020 as compared to total of 4,671 incidents for the same period in 2019, which recorded an increase of 1,026 cases which is equals to 22%. This paper focuses on the technical aspects of various types of cybercrimes concerning the banking units and their related impacts. Additionally, it identifies the threat vectors supporting these crimes and develops measures to aid in combating the resulting cyber-attacks so that such attacks can be better prevented in the future for enhanced security.

2. Literature Review

The review of the literature provides a theoretical basis for emerging threats, as well as a discussion of research issues. What is meant by financial literacy? It is important for all account holders to have knowledge in handling of their financial matters. They could also have a skill and able to manage their financial effectively. What is meant by public awareness? It is where the public to be aware on the cybersecurity awareness, including corporate security awareness, security awareness material on the intranet website, information on screensaver and so on.

Cyber criminals have affected various markets and the banking system is one of them that has encountered various kinds of cyberattacks such as ATM fraud, identity theft, financial fraud, Denial of Service (Raghavan & Parthiban, 2014). The paper discusses the banking sector's cybercrime problem and its impact on bank financial situation. It explores various modes of cybercrime that plague the financial system and the cyber criminals' reasons behind some of these actions. The financial losses in the banking sector are immense globally, both in terms of the fight against cyber-attacks and in terms of the growth of systems.

The internet is already turning into a global network that brings together millions of computers located in different countries and exposes the wide chances of obtaining and exchanging data that so many are now using for illegal acts due to financial problems according to Baker and Glasser (2005), Cybercrime can be categorized as a technology-based crime, a PC and a web-based crime involving governments, commercial enterprises, including global citizens, and cybercrime, a system of piracy, free telephone calls, cyber-bullying, cyber-terrorism and cyber-pornography (Schell & Martin, 2004).

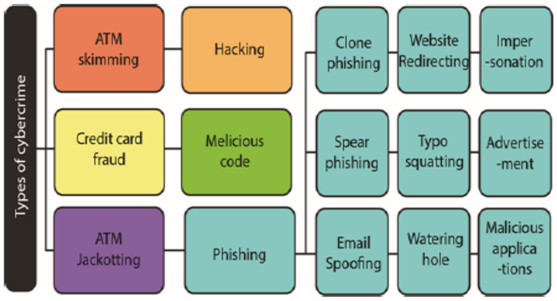

Diagram 3: Type of Cybercrimes in Banking Sector

The knowledge of Internet banking is neglected among too many Southern African banks (Dzomira, 2016). This is shown in diagram 3. On their websites, many companies have developed less than half of the mobile banking fraud awareness available. This indicates that, without comprehensive training of possible internet risks, most cash flow clients take an interest in Internet banking transactions. Most financial clients participate in Internet banking transactions without adequate knowledge of possible internet risks and attacks. As a result, there is a strong probability that Internet banking may be the target of fraud. The banking activities requires full compliance of the standards and best practices in risk management and internal control according to Rameli, Mohd-Sanusi, Mat-Isa, and Omar (2013). As the financial threat is getting susceptible and expensive, the Bank Negara Malaysia (BNM) imposes the intact fraud risk management criteria to ensure the financial risk in banking sectors is mitigated.

New advancement in technology both hard and soft is creating new opportunities for cyber criminals (Santoso, 2012). It is an effective tool for going against the law. In the economic sector, the number of Malaysians opting for online banking to do transaction is increasing. There are 9.8 million online banking account holders in Malaysia. However, cases of online banking scams in Malaysia have been increasing since such first case was registered in 2005. Statistics from Financial Mediation Bureau showed that the number of cases had increased. The effect of cooperation mediated on the relationship between organizational practices, namely, top management commitment (TMC), structured security processes (SSP) and security investment (SI) and cyber security compliance in organizations according to Maslina, Rajah, Mary, David, and Govindamal, (2018). Using data from Malaysia's critical sectors, results show that cooperation mediates TMC and SSP in achieving security compliance. The indirect effect of cooperation on these practices shows its subtle influence, which was not demonstrated in previous studies. These results also support the non-excludable characteristic of cyber security as a public good where cooperation overrides freeriding when security aspects are involved.

The advancements in technology have been at par with the emerging trends and significant changes required in the operations of Indian banking sector. The call for growth has given this unit immense opportunities and as a result, banks are now among the biggest beneficiaries of the IT Revolution. The proliferation in online transactions mounting on technologies like NEFT (National Electronic Fund Transfer), RTGS (Real-Time Gross Settlement), ECS (Electronic Clearing Service) and mobile transactions is a glimpse of the deep- rooted technology in banking and financial matters. But like two sides to a coin, opportunities come with threats and success comes with its equivalent challenges. Thus, with the swift expansion of computers and internet technology, new forms of worldwide crimes known as 'Cyber Crimes' has evolved in the scene. Over time, the nature and pattern of Cyber Crime incidents have become more sophisticated and complex. Banks and Financial Institutions remain the unabated targets of cyber criminals in the last decade. Notably financial gain is still and cybercriminal activities and there is little chance of this changing in the future. Cybercrime continues to be a detrimental problem in South Africa and continues to change in nature and sophistication according to Siyanda and Candice (2019).

Innovations and technological advancements aimed at moving the world towards a digital age increase the risks of cybercrime. Concurrently, as the risk of cybercrime increases so does the challenge to police it. This contributes towards the challenge of detecting, investigating, and combating it. Cyber criminals have intercepted vital and essential government, personal and business information online. These findings suggest that all relevant stakeholder organizations should assist in minimizing the challenge of policing of cybercrime.

There are several theories have been identified and related to the study. Social Learning Theory. is a theory of the learning processes and information behavior that can be attained by observing the behaviors others to acquire new behavior. Behavioral and emotional interpretation occurs thru the interpretation of rewards and punishment, according to Bandura, Ross, and Ross (1963). This process is referred to as vicarious strengthening. The Low Self-Control Theory of Crime. This is the most criminological theories of recent decades as developed by the criminologists. This principle argues that children develop levels of self-control by about seven or eight years of age. During the rest of their lives, this level remains relatively stable. Thus, according to Mark, Greg, and Dikla (2006), this same investigation has concluded that low levels of self-control are correlated with the illegal and impulsive behavior. Citizens are impulsive and insensitive to others, tending to engage in activities that are physical rather than mental. They are having the disability to control their actions, feelings, and emotions. General Strain Theory (GST). According to Agnew (1992), strains increase the probability of crime, especially treatments that are high in magnitude, are seen as unfair, associated with low social control, and create some pressure or rewards for criminal coping.

3. Research Methodology

The research methodology highlights the various methods that will be considered in conducting the research.

3.1. Conceptual Framework

The proposed of theoretical framework in this study which include the 2 independent variables and one dependent variable that show in diagram 4 below:

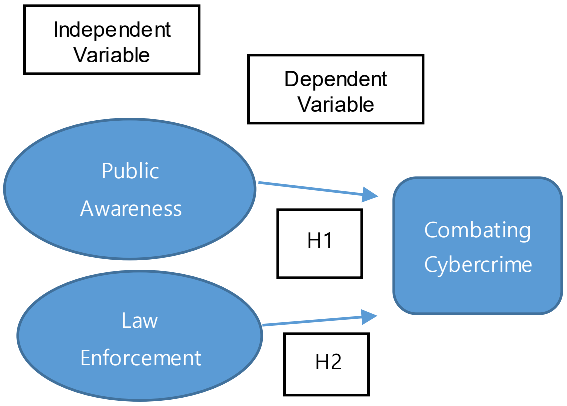

Diagram 4: Proposed Conceptual Framework

3.2. Financial Literacy

It is important in day-to-day lifestyle because it equips customers on knowledge and skills that we need to manage money effectively. Otherwise, with the lack of knowledge, any financial decision made is not success or even face losses to the individual or company. As an institution, it is therefore important to focus on financial knowledge in program will equip staff and clients of banks with the awareness of how they're being tricked to improve these habits. It is also critical to have intelligence with some well threats, regular vulnerability checks performed either by IT security team, including good cyber hygiene overall.

3.3. Public Awareness

As Internet users have increased considerably, so is cybercrime. So, it is the responsibility of one and those that use the internet to be aware of it. Cybercrime and cyber law have been developed to deal with cybercrimes. Various approaches are used to raise cyber security awareness, including corporate security awareness posters, security awareness material on the intranet website, and information on a screensaver, in-class training, videos, simulations and tests. That said, with the increase in cybercrime incidents, there is an urgent need for effective measures to tackle crime.

3.4. Dependent Variable

The dependent variable is clearly stated as combating the financial threat in banking sectors. Each of the Independent Variables will be evaluated through hypothesis respectively. Result of the hypothesis will show the effectiveness of the study whether to accept or reject the proposals. The accepted hypothesis will contribute to the success of the Dependent Variable which is known as Combating the financial threat in banking sectors.

3.5. Hypothesis Development

H1: There a significant positive relationship between the factors of financial literacy on combating the threat of cybercrime in banking sectors.

Questionnaire Dimensions	No. of Items
Questionnaire for Respondent's Profile	7
Questionnaires measuring the relationship between financial literacy on combating the threat of cybercrime.	3
Questionnaires measuring the relationship between public awareness on combating the threat of cybercrime	4
Total	**14**

H2: There a significant positive relationship between the factors of public awareness on combating the threat of cybercrime in banking sectors.

Table 1: Questionnaire Dimensions and Number of Items in Section A and B

The self-administered questionnaires were distributed in a google form of survey and filled up by the respondents. In designing the questions in this survey, the researcher using the close-ended question style, the questionnaire consists of 14 items (questionnaires are available upon request from the main author mohd_yaziz@unirazak.edu.my) complied to the hypothesis and variables, represented in a Likert-scale formatting based on five categories (Strongly disagree, disagree, neutral, agree, strongly agree), the five categories are displayed in numerical form, to make the questionnaire easy and clear for the participants in the questionnaire as follows: 1 strongly disagrees, 2 disagree, 3 neutrals, 4 agree, and 5 strongly agree.

The scale presents the respondents with a set of statements about a person, a thing or a concept and the respondents are required to indicate how strongly they feel, positively or negatively about the statements. The results of Cronbach's Alpha test showed that the invariability degree of the data collection tool in general is 77.3% which is good while the reliability of the sample answers is 87.9% which indicates a high reliability of the results making it possible to generalize the results to the research population. Table 1 below describes and classifies the questionnaires dimensions and number of items for each dimension.

4. Data Analysis

The reliability of the scale preformed in this study was examined through Cronbach's alpha coefficient test. Table 2 below illustrate the results of each questionnaire questions, which distributed according to the study variables.

Table 2: Cronbach's Value of Variables Alpha Test

Variables	Cronbach's Alpha
IV 1: What is the significant relationship between financial literacy on combating the threat of cybercrime	0.78
IV 2: What is the significant relationship between public awareness on combating the threat of cybercrime	0.82

The result in Table 2 shows all the variables and the results of Cronbach's alpha test values greater than 0.7, for measuring the invariability degree for the questionnaire questions. A reliability value of Cronbach's alpha of 0.70 or higher, in general, all parts of the above table came up with high reliability degree. Whereas all of them were of a good degree, where they have reached the highest degree for the questions related to the combating the threat of cybercrime to the study questions is 0.90, which is good for the statistical analysis objectives.

4.1. Descriptive Analysis

Table 3: Demographic Respondents.

Descriptive Analysis	Type	Frequency	Percentage (%)	Total Respondents	(%)
Gender	Male	59	47.6	123	100
	Female	64	52.4		
Age	Below 30 years	14	11.2	123	100
	31 – 40 years	39	32.0		
	41 – 50 years	49	40.0		
	51 – 60 years	21	16.8		
	Above 60 years	0	0		
Academic Qualification	Higher Secondary	19	15.2	123	100
	Graduate	83	67.2		
	Postgraduate	21	17.6		
Working Experience	Below 5 years	8	6.5	123	100
	5 – 10 years	20	16.2		
	11 – 20 years	37	30.1		
	Above 20 years	58	47.2		
Income	Below RM5,000	34	27.2	123	100
	RM5,000 – RM10,000	51	41.6		
	RM10,000 – RM15,000	36	29.6		
	Above RM15,000	2	1.6		
Level of Rank	Clerical	10	8.0	123	100
	Officer	13	10.4		
	Executive	43	35.2		
	Management	57	46.4		
Experience in Cybercrime	Do not know	3	2.4	123	100
	Never	23	18.5		
	Occasionally	42	33.9		
	Often	55	45.2		

The above Table 3 shows the Classification of Respondents Based on Descriptive Analysis which consists of gender of male and female totaling 123 respondents. The result shows that majority of the respondents are female of 64 respondents (52.4%) as compared to men of 59 respondents (47.6%). The researcher has also recorded age type is also one of the demographic profile aspects. Based on the outcomes, there are four categories of age range from below 30 years has showing 14 respondents (11.2%), age from 31 to 40 shows 39 respondents (32%), age from 41 to 50 shows 49 respondents (40%) and lastly age 51 and above which recorded as 21 respondents (16.8%). The qualification background of the respondents is categorized from higher secondary which shows 19 respondents (15.2%), graduate of 83 respondents (67.2%) and 21 respondents (17.6%) under post graduate. Another aspect of demographic profile recorded is working experience in the banking and institution industries. Respondents who were recorded longest time experience of more than 20 years are 58 respondents (47.2%), from 11 to 20 years 37 respondents (30.1%), from 5 to 10 years is 20 respondents (16.2%) and lastly staff who works less than 5 years is 8 respondents (6.5%).

In terms of income background, the respondents who has earned a salary of RM5,000 and below are 27.2% which consist of 34 respondents, range of salary from RM5,000 to RM10,000 is 41.6% for 51 respondents, from RM10,000 to RM20,000 is 29.6% for 36 respondents and those who are earning salary of above RM20,000 is 2 respondents at 1.6%. Level of rank in the organization is also considered under descriptive analysis which consists of rank from clerical which recorded 10 respondents (8%), from officers' category 13 respondents (10.4%), executive of 43 respondents (35.2%) and management level of 57 respondents (46.4%). The last demographical aspect for the research is respondents who have heard, having any knowledge, experienced or even involved in cybercrime. The first category which do not know anything about it shows 3 respondents (2.4%), never had experience or involve in cybercrime at 18.5% for 23 respondents, occasionally heard about it at 33.9% for 42 respondents and often heard or experience at 45.2% for 55 respondents.

4.2. Correlation

Correlation analysis is a statistical tool used to determine the strength of relationship between two quantitative variables. High correlation means that two or more variables have a good relationship with each other, while a weak correlation means that the variables are not very closely related. Thus, the relationship between each variable and its extent towards the mitigating threat of cybercrime are examined through the correlation analysis. A perfect positive correlation has a coefficient of 1.0 and if there is no correlation, it will be denoted by 0.

Table 4: Correlation Coefficient

		IV 1	IV 2
DV 1	Pearson Correlation	.373**	.348**
	Sig. (2-tailed)	<.001	<.001
	N	123	123

**. Correlation is significant at the 0.01 level (2-tailed).
Note:
DV - Combating the threat of cybercrime
IV 1 - Financial Literacy
IV 2 - Public Awareness

Based on Table 4, Correlations it represents the relationship between the IVs towards the DV. This will satisfy the average of the respective independence variables against dependent variable as per research objective. Based on the table 4 above, we can see that all of the IVs are significantly affecting the dependent variable at 0.000. Since the Sig. value or *p*-value must be less than 0.05 (<0.05), the IVs are significantly affecting the dependent variable.

To explain further, the researcher manages to identify the relationship between variables. For Financial Literacy, and Public Awareness, with the relationship in combating the threat of cybercrime are indicated as 0.373, and 0.348, which indicate that the relationship is good, at significant level 0.000. The researcher manages to conclude that the relationships between IVs and DV in this study are strong.

4.3. Hypothesis Analysis

The first IV of Financial Literacy has been stated through hypothesis in this study to evaluate the effectiveness in combating the threat of cybercrime in banking sectors in Malaysia. Regression model has been analyzed as above, the relationship between intent to use debit card is 0.373 at significant value of <0.001. Not only that, the model summary as well as ANOVA also indicated that this IV has positive significant influence towards the DV. Therefore, the hypothesis of H1 is accepted and the H0 is rejected.

The second IV of Public Awareness has been stated through hypothesis in this study to evaluate the effectiveness in combating the threat of cybercrime in banking sectors in Malaysia. Regression model has been analyzed as above, the relationship between intent to use debit card is 0.348 at significant value of <0.001. Not only that, the model summary as well as ANOVA also indicated that this IV has positive significant influence towards the DV. Therefore, the hypothesis of H2 is accepted and H0 is rejected.

Table 5: Results of Hypotheses

Variable	Hypothesis	Results
Financial Literacy	The financial literacy has a significant relationship to combating the threat of cybercrime in banking system	Accepted
Public Awareness	The public awareness has a significant relationship to combating the threat of cybercrime in banking system	Accepted

The research findings show some hypotheses analysis in this research such as Table 5 summarizes all hypotheses with the IVs which have been tested their significant level towards DV.

5. Conclusion

Based on the output the researcher concludes that all tested hypotheses are acceptable, all null hypotheses are rejected as all of the variables are significant at p-value <0.001. Thus, the researcher concluded that all independent variables; have significant influence towards the dependent variable in this study.

Based on the research finding and the interview with 123 respondents, the researcher found from the discussion and feedback from their overview that there regarding the pros and cons of cybercrime. There are many challenges in front of us to fight against the cybercrime. It is increasing day by day, and with the growing technology, they may not be able to be completely eradicated (Krishna & Purandare, 2021). Some of the challenges remained are:

a. Lack of awareness and the culture of cyber security, at individual as well as organizational level.

b. Lack of trained and qualified manpower to implement the counter measures.

c. No e-mail account policy especially for the defense forces, police, and the security agency personnel.

d. Cyberattacks have come not only from terrorists but also from neighboring countries contrary to our National interests.

e. The minimum necessary eligibility to join the police does not include any knowledge of computers sector so that they are almost illiterate to cyber-crime.

f. The speed of cyber technology changes always beats the progress of govt. sector so that they are not able to identify the origin of these cyber-crimes.

g. Promotion of Research & Development in ICTs is not up to the mark.

h. Security forces and Law enforcement personnel are not equipped to address high-tech crimes.

i. Present protocols are not self-sufficient, which identifies the investigative responsibility for crimes that stretch internationally.

j. Budgets for security purpose by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compared to other crimes.

As there is no specific enforcement related to the law, the major impact of these crimes is left unsolved. There should be fast track mobile courts to solve these cases, to meet the grievances and build confidence. The law enforcement should be very rigid and updated from time to time to keep a track of such crimes. Many a times, an act has to be enforced to curb this kind of track on the operating network activities with the help of Big Data among the public. Punishments and penalties need to be exercised thoroughly to minimize the impact of these issues. Banks Awareness Program should be initiated to inform the public about the ongoing scenario and to penalize the attackers. The public should report these cases to the Cyber Crime Branch in the matters related rather than just an upcoming threat. By referring it to the banks, to ensure fast and strict actions. Although high-profile cyberattacks, such as ransomware, have been garnering a lot of attention from enterprises, the study found that for organizations in Malaysia that have encountered cybersecurity incidents, data exfiltration and data.

The government should also keep a track on the operating network activities with the help of Big Data among the public. Punishments and penalties need to be exercised thoroughly to minimize the impact of these issues. Banks Awareness Programs should be initiated to inform the public about the ongoing scenario and to penalize the attackers. The public should report these cases to the Cyber Crime Branch in the matters related rather than just an upcoming threat. By referring it to the banks, to ensure fast and strict actions. Although high-profile cyberattacks, such as ransomware, have been garnering a lot of attention from enterprises, the study found that for organizations in Malaysia that have encountered cybersecurity incidents, data exfiltration and data corruption are the biggest concerns as they have the highest impact with the slowest recovery time.

Recommendations to the future researchers

Lessons learnt the researcher has to take initiative to spend time with the Information Technology's team in the banks to study the actual situation faced by their team in combating the cybercrime from attacking the banks. Sometimes, the situation faced by them will not be the same as what we observe.

A multi-vocal literature review for Law-enforcement agencies to combat cybercrime and cyber threats effectively is proposed by Cascavilla, Tamburri, and Van Den Heuve (2021)

Other than that, the researcher should also identify non-banking operations group e.g. Information Technology's team, Risk Management, Compliance and Audit Team to be a part of respondents beside branch staff. With this, the researcher will get the real and accurate result in doing the research deep from the actual source.

References

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. Criminology, *30*(1), 47-88.

Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behaviour in e-Banking services. International Journal of e-Education, e-Business, e-Management and e-Learning, *7*(1), 70-78.

Baker, P., & Glasser, S. (2005). Kremlin rising: Vladimir Putin's Russia and the end of revolution. New York, NY: Scribner.

Bandura, A., Ross, D., & Ross, S. A. (1963). Vicarious reinforcement and imitative learning. The Journal of Abnormal and Social Psychology, *67*(6), 601–607.

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. Thousand Oaks, CA: Sage Publications.

Cascavilla, G., Tamburri, D.A., and Van Den Heuvel, W.-J. (2021), Cybercrime threat intelligence: A systematic multi-vocal literature review, Computers and Security, 1-29.

Check, J., & Schutt, R. K. (2012). Teacher research and action research. Research methods in education, 255-271.

Chen, C. W. (2014). Are workers more likely to be deviant than managers? A cross-national analysis. Journal of Business Ethics, *123*(2), 221-233.

Collins, N. L., & Miller, L. C. (1994). Self-disclosure and liking: a meta-analytic review. Psychological bulletin, 116(3), 457-475.

Connelly, L. M. (2008). Pilot studies. Medsurg Nursing, *17*(6), 411-412.

Dzomira, S. (2016). Espousal of combined assurance model in South Africa's public sector. Public and Municipal Finance, *5*(4), 23-30.

Farhana, S. (2020, October 25). The rise of cybercrime in Malaysia - what you need to avoid. Astro AWANI Television Network.

Felson, M., & Cohen, L. E. (2017). Human ecology and crime: A routine activity approach. In Crime Opportunity Theories, (pp. 73-90), Oxfordshire, England: UK.

Gordon, L.A. & Loeb, M.P. (2003). A Framework for Using Insurance for Cyber-Risk Management. Communications of the ACM, *46*(3), 81–85.

Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. Palo Alto, CA: Stanford University Press.

Gupta, S. (2012). Buffer overflow attack. IOSR Journal of Computer Engineering, *1*(1), 10-23.

Hill, J. B., & Marion, N. E. (2016). Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century. Westport, CT: Praeger Publishers.

Hill, R. (1998). The mathematical theory of plasticity. Oxford,UK: Oxford University press.

Isaac, S., & Michael, W. B. (1995). Handbook in research and evaluation: A collection of principles, methods, and strategies useful in the planning, design, and evaluation of studies in education and the behavioral sciences. Washington, DC: American Psychological Association.

Johanson, G. A., & Brooks, G. P. (2010). Initial scale development: sample size for pilot studies. Educational and psychological measurement, *70*(3), 394-400.

Khalid, K., Abdullah, H. H., & Kumar M, D. (2012). Get along with quantitative research process. International Journal of Research in Management, 79-88.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and psychological measurement, *30*(3), 607-610.

Krishna V. V., & Purandare, P. A Qualitative Research on the Impact and Challenges of Cybercrimes (2021), Journal of Physics: Conference Series, 1-12.

Kuder, G. F., & Richardson, M. W. (1937). The theory of the estimation of test reliability. Psychometrika, *2*(3), 151-160.

Lakomski, G. (2001). Organizational change, leadership and learning: culture as cognitive process. International Journal of Educational Management. 79-88.

Lowry, R. (2014). Concepts and applications of inferential statistics. Computer Science.

Mark M., Greg P, & Dikla S, (2006) Self-control depletion and the general theory of crime Journal of Quantitative Criminology, *22*, 263-277.

Maslina D., Rajah R., Mary G., David A. & Govindamal T. (2018). Bridging the gap between organizational practices and cyber security compliance: Can cooperation promote compliance in organizations? International Journal of Business and Society, *19*(1), 161-180.

Nachmias, D. (1972). Political alienation and political behavior. Oxfordshire,UK: Routledge.

Neuman, S. B., & Roskos, K. (1997). Literacy knowledge in practice: Contexts of participation for young writers and readers. Reading Research Quarterly, *32*(1), 10-32.

Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). NY: McGraw-Hill.

Ponto, J. (2015). Understanding and evaluating survey research. Journal of the advanced practitioner in oncology, *6*(2), 168-171.

Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. International Journal of Current Research & Academic Review, *2*(2), 173-178.

Rameli, M. N. F., Mohd-Sanusi, Z., Mat-Isa, Y., & Omar, N. (2013). Fraud occurrences in bank branches: The importance of internal control and risk management. The 5th International Conference on Financial Criminology (ICFC). (p. 77-89). May 28-29, Kuala Lumpur, Malaysia.

Rubin, D. S., & Levin, R. I. (1998). Statistics for management. Language, *16*(1026p), 25.

Santoso, Edy (2012), Consumer Protection for Online Banking Scams via e-mail in Malaysia, UUM Journal of Legal Studies, *3*, 1-22.

Schell, B. H., & Martin, C. (2004). Cybercrime: A reference handbook. Santa Barbara, CA: ABC- CLIO.

Singh, J., & Singh, H. (2012). Continuous improvement approach: state-of-art review and future implications. International Journal of Lean Six Sigma. *3* (2), 88-111.

Singleton, R. A., & Straits, B. C. (2012). Survey interviewing. In SAGE handbook of interview research: The complexity of the craft, (pp. 77-98), Newcastle upon Tyne, UK: Sage Publications.

Siyanda Dlamini & Candice Mbambo (2019). Understanding policing of cyber-crime in South Africa: The phenomena, challenges and effective responses, Cogent Social Sciences, 5:1, DOI: 10.1080/23311886.2019.1675404

Suter, W. N. (2012). Qualitative data, analysis, and design. Introduction to educational research: A critical thinking approach, *2*, 342-386.

Vladimir. G., (2005). International cooperation in fighting cybercrime. [Online]. Available: https://www.crime-research.org/articles/Golubev0405

Xu, J., & Gordon, J. I. (2003). Honor thy symbionts. Proceedings of the National Academy of Sciences, *100*(18), 0452-10459.