**International Journal of Academic Pedagogical Research (IJAPR)**
**ISSN: 2643-9123**
**Vol. 10 Issue 1 January - 2026, Pages: 71-89**

# An Empirical Study On Cybercrime Awareness: The Emerging Threat To Banking Sectors In Malaysia

**Wan Nora Binti Wan Ibrahim1, Mohd Yaziz bin Mohd Isa2, Mustafa Bin Dakian3**

1Tun Abdul Razak Graduate School (TRGS), Universiti Tun Abdul Razak (UNIRAZAK), Kuala Lumpur
norawibrahim@gmail.com
2Lecturer at Tun Abdul Razak Graduate School (TRGS), Universiti Tun Abdul Razak (UNIRAZAK), Kuala Lumpur
**mohd_yaziz@unirazak.edu.my**
3Lecturer at Tun Abdul Razak Graduate School (TRGS), Universiti Tun Abdul Razak (UNIRAZAK), Kuala Lumpur
mustafadakian@gmail.com

**ABSTRACT: Purpose**: The purpose of this study is to analyze the empirical study on cybercrime, an emerging threat to banking sectors in Malaysia. This study investigates the significant contribution of financial literacy, public awareness, ICT and technical tools, education and law enforcement on the relationship of cybercrimes and combating the threat of cybercrime. **Design/methodology/approach**: The impact of cybercrime incidents on organizational performance is investigated by further exploring the moderating effects of effectiveness on combating the threat of cybercrime. A sample of 123 banks employees from 12 commercial banks in Malaysia was studied by using research survey design. The cross-sectional research approach was applied with using the random sampling design with 123 respondents were participated in this study. **Findings:** The financial literacy, public awareness, ICT and technical tools, education and law enforcement incidents have negative/positive impact on organizational performance effectiveness to combating the threat of cybercrime. Some recommendations also proposed from research finding, banking industry and government regulations. **Limitations/implications**: The present study focus on banking sector so its finding cannot be generalized in other sectors. Further in depth comparative studies in other sectors with different cultural and SOP policy reinforcement settings will help to authenticate the research findings. **Practical implications:** Information security and public awareness weakens the negative impact of cybercrimes on combating the threat of cybercrime, therefore it is important for banks' PR managers to set up more security financial literacy and education to increase customers' awareness on cybercrimes. **Originality/value:** Linking these topics has created a new study within the combating the threat of cybercrimes in Malaysia. The present study also enhances the understanding of customers' role to combat the impact of cybercrimes on the banking industry performances.

**Keywords** - Cybercrime, public awareness, banking sectors, organizational performance, internet security system, criminal technology

## 1. INTRODUCTION

In modern computer technologies and data networks, people are seldom to rob money from the vault because lots of money exists in cyber space. Banks have to 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 of all places in the world. It is on the rise with cyber-criminals taking advantage of 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, government departments, school, universities as well as public individually. In Malaysia, it has been reported to be more lucrative crime than drug trafficking. It is reported that cybercrime contributes 70% of the whole commercial crimes' cases. The total losses recorded with regards to the cybercrime were RM305 million and RM247 million for year 2019 and 2020 respectively as declared by Malaysian Crime Prevention Foundation (MCPF).

There is various type of cybercrimes. Some of the more common type of cybercrime include but are not limited to: DDOS Attacks, Botnet, and Identity Theft. 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 extorting (demanding money to avoid a threatened attack) and cyber criminals are other forms of cybercrimes (a type 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).

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 the unauthorized access and use the financial information for purpose of fraud. These techniques and tactics are highlighted in this study. It is important for all users to understand the potential crimes and effect the day-to-day life.

### 1.1. Online Banking's Customer's Behavior Measurement

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, email 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 et al. (2003). In 2020, statistics provided by the Malaysian Computer Emergency Response Team (MyCERT) recorded 8,366 cases of cybercrime incidents from January to September 2020.

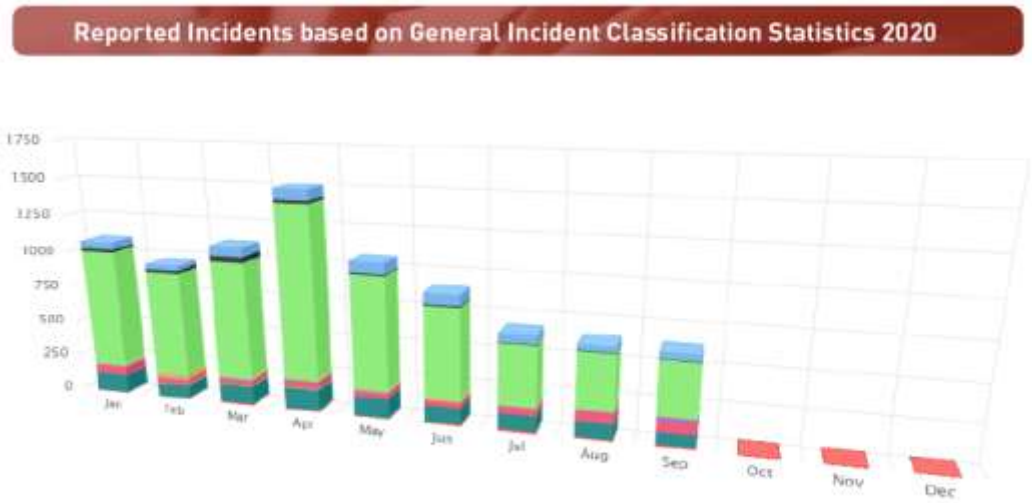


*Figure 1: Reported Incidents based on General Incident Classification Statistics 2020 – MyCERT*

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%. Cases have risen since the introduction of the Movement of Control Order (MCO) from Pandemic Covid19 in March 2020. Started from 18 March to 30 June 2020, Cyber999 Help Centre had recorded a total of 3,906 complaints lodged by all sectors in Malaysia, an increase of more than 90% as compared to 2019. The reported cases involved cyberbullying, fraud, cyber intrusions, hacking attempts and spam, most of which occurred in urban areas with a high-speed Internet connection (Hill & Marion, 2016).

Under the Ministry of Multimedia and Communications (MCMC), Cybersecurity Malaysia is established as a cyber security specialist agency to provide a broad range of services and strengthen Malaysia's self-reliance in cyberspace. The organization assists enforcement agencies in cyber forensics and analysis, such as analyzing evidence and providing expert witnesses for relevant cybercrime cases. It also aims to establish a culture of security through awareness programmes and best practices among children, teenagers, parents and organizations.

Besides Cybersecurity Malaysia, MCMC is also multiple sub-organizations and services provided to cater to Malaysia's growing need for online security. There also exist many cyber laws and policies such as the Computer Crime Act 1997 and the Communication and Multimedia Act 1998 that act as a safeguard against cyber-criminal activities in the country. That with the rise in cybercrime cases, there is an urgent need for proactive steps to tackle the crime. Cybersecurity Malaysia for example has

highlighted the shortcoming of its agency in the lack of cyber security professionals. Hence, universities are urged to offer more courses and programmes to educate the public and create awareness on cyber security. More recently, a proposal has also been submitted by the MCPF for the government to set up a committee consisting of the police, MCMC, Bank Negara, telecommunication companies and National Cyber Security Agency to discuss, monitor and identify effective actions to address issues of cybercrime (Astro AWANI, 2020).

Cybercrime has given huge impact to banking sectors in Malaysia, in terms of cost to be borne by the banks on the damage of security system, economic as well as to jeopardize the image and credibility of banking institution. In order, to mitigate the emerging threat in banking sectors, banking institutions in Malaysia have implemented strategies in upgrading the Information Technology System, public awareness in dealing with financial transactions and to equip all banks staff with cybercriminals knowledge from time to time. The Bank Negara Malaysia as well as MCMC should come out with the blueprint of mitigating the cyberthreat respectively.

### 1.2. Problem Statement

The Government of Malaysia as well as Bank Negara Malaysia through all commercial banks in Malaysia have aggressively promoting the development of e-banking (digital banking). In order, to deliver fast and efficient banking services to all categories of customers. The transactions will use a medium of digital channels with minimal brick-and-mortar presence. However, cybercrime remains rampant with cyber-criminals taking advantage of new digital technologies. Information technology growth and cybercrime are simultaneous. This study will focus the public awareness on cybercrime: an emerging threat to banking sectors in Malaysia. The main issues are to evaluate the public awareness on cybercrime methodology. Computer criminals are always seeking unpermitted access to confidential data or financial falsified activity information. The implications of the rising cybercrime wave make it appear to be Malaysia's 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 both developed and developing nations.

As for the banking sectors, the Information Communication Technology plays an important role in mitigating the cybercrime. Customers of banks have to be consistently reminded of public awareness among banking customers of how to avoid the threats available. To establish a culture of security and that of other children, young people, parents and institutions through community awareness and best practices. There is a need for the Government of Malaysia to review the current law of PDRM on Computer Crime Act and Evidence Act, Penal Code, to activate the Local Agency Task Force, promoting the Awareness Campaigns, tighten the role of Police Cyber Investigation Response Centre (PCIRC), to be supported by Mobile Intelligence System (MIS).

An initiative involving money, time and energy has been made to develop corporate governance practices, internal control mechanisms, risk management techniques and training of staff to address the problems. The fraudsters, however, are knowledgeable individuals who often introduce high-technology initiatives in order to achieve their target and easily earn significant returns from illegal activities. In getting access to the wealth and assets of individuals or organizations, they may also look for ways to override the mechanisms or deceive decent citizens as victims. The tragic fact is that most organizations still make an attempt to properly recognize the real risks associated in fraud as a victim, and little effort made to identify and deter fraud until it happens. The objective of this study is not only way to tackle cybercrime is to establish a prevention method 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 avoiding losses of revenue and assets, but also to enhance the efficiency of commercial banks and the overall credibility in the business setting.

The Information Communication Technology (ICT) has revolutionized a different facets of human life that have simplified of our lives. It has been used by various all types of levels, sectors and industries, which has the formatted standard of streamlining the work process through sorting, summarizing, coding and customizing. Nonetheless, ICT brings unintended effects about the forms of numerous cybercrimes. Cybercrimes have impacted numerous industries and one of the banking sectors is the banking industry.

Microsoft Inc. in collaboration with Frost & Sullivan stated the critical issues of its study titled “Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World”. The study reveals that the potential economic loss in Malaysia due to cybersecurity incidents can hit a staggering **US$12.2 billion.** This is **more than 4 percent** of Malaysia’s total GDP of US$296 billion. The study aims to provide business and IT decision makers with insights on the economic cost of cybersecurity breaches in the region and identify the gaps in organizations’ cybersecurity strategies. The study involved a survey of 1,300 business and IT decision makers ranging from mid-sized organizations (250 to 499 employees) to large-sized organizations (more than 500 employees). The study reveals that more than half of the organizations surveyed in Malaysia

have either experienced a cybersecurity incident (17%) or are not sure if they had one as they have not performed proper forensics or data breach assessment (36%) (Microsoft Malaysia, 2018).

Those who have encountered various types of cybercrime, such as ATM theft, phishing, theft of identification, service denial. The paper talks about issues of cybercrime in the banking sectors. It evaluates the scenario of cybercrime and determines the person involved in the scenario. The same also addresses the various forms of cybercrime that plague the financial sectors and reasons behind such actions by cyber criminals. The financial sectors especially banking, are immense around the globe in terms of both combating cyber threats and research design so that such attacks can be eliminated in the future. This paper will contribute the knowledge of cybercrime and the emerging threat in banking sectors in Malaysia. The study revealed that: 1) A large-sized organization Malaysia can possibly incur an economic loss of US$22.8 million, more than 630 times higher than the average economic loss for a mid-sized organization (US$36,000); and 2) Cybersecurity attacks have resulted in job losses across different functions in three in five (61%) of organizations that have experienced an incident over the last 12 months.

To calculate the cost of cybercrime, Frost & Sullivan has created an economic loss model based on macro-economic data and insights shared by the survey respondents. This model factors in three kinds of losses which could be incurred due to a cybersecurity breach: 1) Direct: Financial losses associated with a cybersecurity incident – this includes loss of productivity, fines, remediation cost, etc; 2) Indirect: The opportunity cost to the organization such as customer churn due to reputation loss; and 3) Induced: The impact of cyber breach to the broader ecosystem and economy, such as the decrease in consumer and enterprise spending.

The implications from the theoretical and practical perspective are to avert on going massive losses owing to cybercrime, the researcher quest for development of an alert system that can create the awareness of both the banks and the customers by effectively implementing and integrating big data technology into their system to mitigate the negative impacts of cybercrime. The contribution of this study is confirms an increasing wave of cybercrime that has impacted negatively on the goodwill and economic growth of financial institutions, indirectly through loss of trust in the digital infrastructure or directly through fraud and extortion to banking industry in Malaysia.

### 1.3. Research Objectives

The main general objective of this study is to investigate the public awareness on cybercrime that an emerging threat to banking sectors in Malaysia. In line with the main of research objectives stated the following of specific objectives;

1.3.1. To analyze the public awareness on cybercrime an emerging among customers banking sectors in Malaysia

1.3.2. To investigate the relationship between the factor of financial literacy on combating the threat of cybercrime in banking sectors.

1.3.3. To investigate the relationship between the factor of public awareness on combating the threat of cybercrime in banking sectors.

1.3.4. To investigate the relationship between the factor of Information Technology Communication (ICT) tools and Prevention Techniques on combating the threat of cybercrime in banking sectors.

1.3.5. To investigate the relationship between the factor of education on combating the threat of cybercrime in banking sectors.

1.3.6. To investigate the relationship between the factor of law enforcement on combating the threat of cybercrime in banking sectors.

1.3.7. To propose the strategies and solutions for the enhancing the public awareness on cybercrime that an emerging threat to banking sectors in Malaysia.

## 2.0. EMPIRICAL RESEARCH

The review of the literature provides a theoretical basis for emerging threats, as well as a discussion of research issues. An example of the previous research that has been done related to the study of this subject matter by Raghavan and Parthiban (2014), 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, clearly described on their paper. 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.

According to Baker and Glasser (2005), 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. Nigeria, as a third-world nation, faces a variety of financial challenges in cases of corruption, unemployment, poverty and so on which makes crime a thrive. In general, the chapter addresses previous studies on ICT tools and the definition of cybercrime by highlighting its connection with this study based on the research issues mentioned above and the objectives of the study. This chapter points out the theoretical part of the effect of cybercrime on the online banking system, which has been a topic of concern for many decades, and which varies from one another.

Schell and Martin (2004) were characterized cybercrime 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.


*Diagram 1: Type of cybercrimes in banking sector*

Based on diagram 1 above as previous research by Dzomira (2016), as reflected above in this findings, it concludes that knowledge of Internet banking neglect on the part of too many Southern African banks is very poor. 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. This indicates that 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 as conveyed by Rameli, Mohd-Sanusi, Mat-Isa and Omar (2013). As the financial threat is getting susceptible and expensive, the Bank Negara Malaysia has to impose the intact fraud risk management criteria to ensure the financial risk in banking sectors is mitigated. All level of staff in banking sectors especially the frontlineras well as the senior management level have to be provided a strategic initiative in protecting of any illegal activities which may jeopardize their performance of work.

Threat exists as a result of vulnerabilities in the monitoring of banking operations. Therefore, to include the formation of information and communication technologies, include the use of a rate of loading screening system, concerted approaches to solve any weaknesses in internal control system should be intensified. In their standard operating procedure, scammers are becoming much more comprehensive, and financial companies need to be a few years ahead of them in the fight against fraud.

### 2.1. Conceptual Framework

The proposed of conceptual framework in this study which include the 5 independent variables and one dependent variable that show in diagram 2 below:

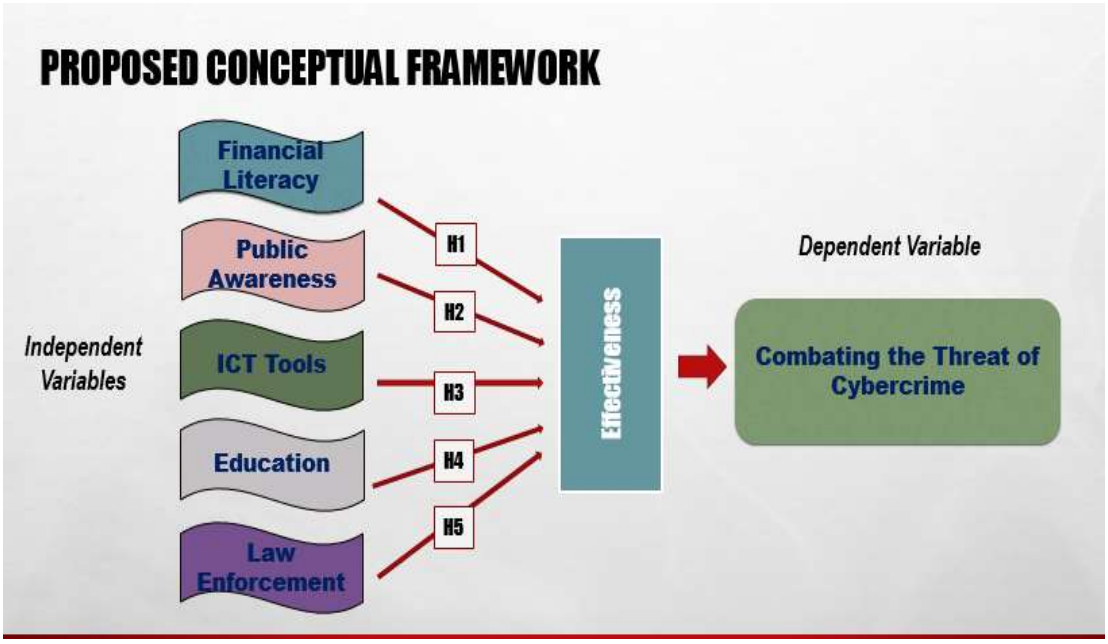


*Diagram 2: Proposed Conceptual Framework*

The above is the proposed Conceptual Framework suggested in this study which constructed by element of independent variables, hypothesis and a dependent variable. This framework will help to identify the problem by using a broad set of ideas and theories. It illustrates what we expect from the research and define the relevant variables in the study to map out how it relates each other. It is constructed prior to collection of data and represented in a visual format. In this research, the proposed Conceptual Framework draws the imposition of five (5) Independent Variables consists of:

## 2.2. Operational and Measurement

### 2.2.1. Independent Variables

In science, the alternative hypothesis is the cause. In your analysis, its value is independently of other indicators. The affect is the primary outcome. Its value is dependent on the individual variable's adjustments. As per item *Diagram 3*, the followings are five (5) construct of independent variables identified in the study;

### 2.2.2. 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 in order 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. Without saying the awareness and training are important, when exploits happened, there will always be a human error. These things have to be considered when there is an individual approach:

- To be alert and alert and vigilant when shopping online, making any payment or deposits, or logging in to your online bank and government portals.
- In making any payments and transactions via official sites, to ensure who is the recipient to receive the money and on what purpose.
- Be careful in clicking any links provided in the question, check the name the sender and, if in doubt, ask for a second opinion.

### 2.2.3. 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. Cyber Security Malaysia, for example, has highlighted the shortage of cyber security experts in its agency. Universities are also encouraged to deliver more courses and services to educate the public and raise awareness about cyber security.

### 2.2.4. Information Communication Technology (ICT)

Diagram 3 below is access to information and communication technology (ICT), cybersecurity and social development are connected. For people to gain information and skills and to use them for their own purposes and for society, ICT offers an unparalleled opportunity. The international dimension of cybercrime is reflected in the strategies adopted by ICT regulators to promote cybersecurity. Governments have to seek to harmonize national legislation, regulations, standards and guidelines with a view to creating effective regional and international frameworks for combating cybercrime.

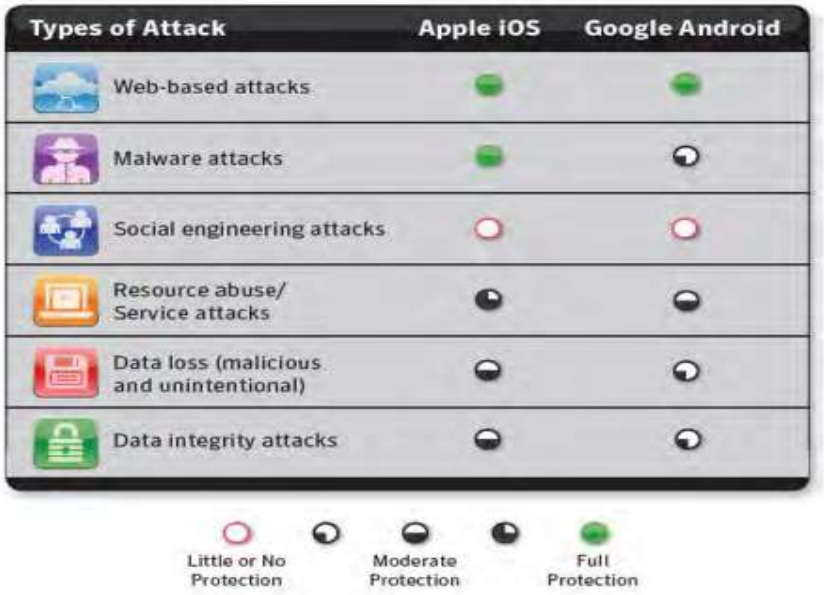


*Diagram 3: Mobile Platform Security Summary*

The Internet of Things (IoT) boom means that there are more data points to be monitored and entered into the networks. The use of machine learning and artificial intelligence (AI) will help to solve this issue while at the same time alleviating the skills gap. These technologies are capable of collecting and analyzing data, tracing risks, identifying vulnerabilities, reacting to breaches, and thus reducing the number of vulnerabilities. The advantages that the technology can bring to banking sectors are;

- **Prevention -** With the artificial intelligence, the program can be developed to deploy solutions in real time and to search for security flaws.
- **Detection -** Artificial intelligence would help the cybersecurity analysts in detecting the high risks incidents. It also help to investigate the threats.
- **Response - Artificial intelligence and m**achine learning will separate the networks features into the isolate assets or to redirect attackers away from valuable data and vulnerabilities.

**The most important: All banks have to choose the reliable and right cybersecurity solution for the bank respectively.**

### 2.2.4. Education Ecosystem / Training

While cyber security threats can be frightening and require vigilance, the public is not fighting these threats on their own. The best way for bank employees to advise financial banking users to protect their data and make sensible use of devices. The bank needs

to invest in Employee Training to make cyber security awareness a priority. Employees must be trained to recognize phishing and social engineering. In order to avoid any attempt on the criminal or fraud, the staff especially the front line should be equipped with knowledge and to carry out the precaution measures of "Know Your Customer (KYC)', 'Customer Due Diligence (CDD)', and 'Enhanced Customer Due Diligence (ECDD)' It has to be implemented in day to day worklife.

Training is all there is to do with cyber security. There is a steady increase in new threats, and the bank needs to place its workers in a way that is sustainable. Even when they are asked to exchange login details, they want to be in the habit of checking critically. Once in a quarter and more, bank personnel should be prepared with occasional 'live fire' training exercises and frequent reminders of the threats that have evolved and vulnerabilities that occur. The cyber security employee policy is the key resource that employee can access of they have any doubts about the cyber security. It includes all aspects of training, as well as the company policies and the best practices.

### 2.2.5. Law Enforcement

It plays a key role in implementing the cyber security priorities of our nation by examining a wide variety of cybercrimes, including fraudulent activity to child violence, arrest and imprisonment. Usually, when a complaint is filed with the police, the law enforcement authority reaches out to the entity or platform on which the hacking incident occurred. The Internet protocol address of the hacker is traceable to the police and the investigation is forwarded on the basis of the cyber cell article. The face of law enforcement has also been transformed by technological changes. Improvements in enforcement technologies make it more difficult for officials to raise public visibility, from drones to body - worn cameras to GPS that have and thermal imaging devices.

In Malaysia, the law enforcement should be introduced to include government policies such as the Cyber Crime Act 1997 and the Communications and Multimedia Act 1998. The Act is being introduced to protect against cyber-criminal activities in the region. Cyber Security Malaysia has to play important role in highlighting the shortcoming of its agency due to the shortage of cyber security professionals. A proposal has to be submitted by MCPF requests to the Government to set up a committee consisting of the police, MCMC, Bank Negara, telecommunications companies and the National Cyber Security Agency to examine, track and identify successful actions to resolve cybercrime issues.

The questionnaire was numerous references to ensure that when data collection is carried out, the questions are correct. The pre-test feedback is used to determine the accuracy of the questionnaire. The data will be collected through drop and pick by the investigator when the respondents is doing financial transactions in the banks, at them place of work, execute the questions and where appropriate collect them the very next day. The questionnaires are now used to compile answers as reliably as possible from the respondents. Only short answers, checkboxes and Likert scale will be used.

### 2.2.6. Mediating Variable

Mediating variables is a cause-and-effect relationship, a variable that links the independent variables and dependent variables. It allows the relationship between them to be better explained. As per item 2.4 Conceptual Framework, the mediating variable mentioned is 'effectiveness'. On a clearer description of an observation, observation or problem that can be tested by more study and/or evaluation, the efficacy of the appropriate interpretation is to be assessed. A clearly defined and supportable assumption of an occurrence should be an efficient hypothesis.

### 2.2.7. Dependent Variable

A dependent variable of this study is the variable in the statistical modelling or experimental science that depends on other factors it will be measured. The variables will be change as a result of an experimental manipulation of the independent variables. It also appears as the presumed effect. In this research, the dependent variable is clearly stated and read as 'combating the financial threat in banking sectors'. It means an effort of research will be carried out through the comprehensive research methodology and to meet the objective of the research. Objective of dependent variable is met if research on mechanism and factors to be mitigated on financial threat in banking sectors in Malaysia. Through the study and research methodology, cases of financial and property losses can be combated in banking industries in Malaysia. In other words, the purpose of research is succeed and can be proposed in the banking sectors as well as the Bank Negara Malaysia in implemented the intact security levels and other government initiatives.

## 3.0. RESEARCH METHODOLOGY

### 3.1. Research Design

In this research, the Cross-Sectional design types was chosen. This design is often identified with questionnaire research, a method of data collection common in many social science fields. Though the cross-sectional design would allow to assess the relation (or correlation) between financial literacy, public awareness, ICT and technical tools, education and law enforcement to combating the threat of cybercrime. The main advantage of cross-sectional studies it permits researchers to employ random probability samples. Cross Sectional studies are also used to infer causation. Besides that, such studies are having subjects are neither deliberately exposed, treated nor not treated and hence there are seldom ethical difficulties. Only one group is used, data are collected only once and multiple outcomes can be studied; thus, this type of study is relatively cheap. This research is supported by secondary data collected from the selected banking industry.

### 3.2. Population

According to Denzin and Lincoln (2014), the population in the sample is a set of people or elements that are subject to a test to make inferences. The population would be based on bank clients from Pahang who have experience in cybercrime, consisting of clients of banks as well as employees of banks.

### 3.3. Sample

The sample research is a type of selection process for primary study components and analysis is determined to address the research questions as identified by Gaylord and Galliher (2012). The analysis process of this subset is called sampling, namely research take several examples of population study named samples. Generally, a sample is the selected item or represent to population studies. Samples that will be selected must represent a population study so that the findings can be made revenue generation that is able to provide a comprehensive interpretation of the population. Therefore, the number of small samples can be taken in each group and this gives more precision in the random sampling. This study using cluster sampling (local random sampling) because the cluster method to ensure that the sample accurately represents the whole population. The target participants for this research is 123 respondents who have experience on cybercrime were randomly selected who are responding by using google form of questionnaires.

### 3.4. Data collections

The self-administered questionnaires were distributed in a google form of survey and filled up by the respondents. The data collections were completed with the assistance of some colleagues of the researcher. Work process to obtain data when each respondent is required to reply to a google form questionnaire in the same way as all respondents can be considered a class. The google form questionnaire has been added with the accompanying letter as a reference to the purpose of the study and asks the respondents to provide sincere answers and no bias, as included. This research was carried out with the manager of the company, which the researcher has been working experience since 1991. This facilitated the process of distributing and receiving the reply google from the respondents at each department using the banking online system frequently. The different groups of the respondents were given three weeks from 16 April 2021 until 07 May 2021. Then data was coded and the statistical package for social sciences (SPSS) is used as it is one of the most standard and extensively available software packages for preparation and executing computerized data analysis.

### 3.5. Data Collections

*Table 1* below show the total respondents of the study. In this study, the total respondents were 123 persons. The google form of questionnaire survey is distributed from 16 April 2021 until 07 May 2021, there are 123 respondents are responding.

*Table 1: Total Respondents of the Study*

| Areas | Total Questionnaire Distributed | Total Questionnaire Received |
|---|---|---|

| | | |
|---|---|---|
| • Affin Bank Berhad<br>• Agro Bank Berhad<br>• Alliance Bank Berhad<br>• Ambank (M) Berhad<br>• Bank Islam Malaysia Berhad<br>• Bank Kerjasama Rakyat M Berhad<br>• Bank Simpanan Nasional<br>• Bank Muamalat Malaysia Berhad<br>• CIMB Bank Berhad<br>• Hong Leong Bank Berhad<br>• HSBC Bank Berhad<br>• Maybank Berhad<br>• RHB Bank Berhad<br>• UOB Bank Berhad<br>• Public Bank Berhad | Google Form forwarded to BMs of 15 Banks under Association of Bank Malaysia, Terengganu State | 123 |
| **Total** | | **123** |

## 4.0. DATA ANALYSIS AND RESEARCH FINDINGS

### 4.1. Reliability Test

The reliability of a research instruments will concern the extent to which the instrument yields the same results on repeated trials. The tendency toward consistency found in repeated measurements is referred to as reliability (Carmines & Zeller, 1979). Reliability is defined as the extent to which a questionnaire test observation or any measurement procedure produces the same results on repeated trials. In short, it is the stability or consistency of scores over time or across raters. There are three aspects of reliability, namely: equivalence, stability and internal consistency (homogeneity). It is important to understand the distinction between these three as it will guide one in the proper assessment of reliability given the research protocol. The first aspect is element of equivalence to measure through a parallel forms procedure in which one administers alternative forms of the same measure to either the same group or different group of respondents. The second aspect is reliability and stability to occur when the same or similar scores are obtained with repeated testing with the same group of respondents. The third aspect is reliability is internal consistency (or homogeneity that concerns the extent to which items on the test or instrument are measuring the same thing.

Internal consistency is estimated via the split-half reliability index, coefficient alpha (Cronbach, 1951) index specifically, coefficient alpha is typically used during scale development with items that have several response options (i.e., 1 = strongly disagree to 5 = strongly agree) or the Kuder-Richardson formula 20 (KR-20) (Kuder & Richardson, 1937) Index. The popular and commonly used method to assess and estimate internal consistency is Cronbach's Alpha. The general convention in research has been explained by Nunnally and Bernstein (1994) who state that one should strive for reliability values of 0.70 or higher.

The reliability of the scale preformed in this study was examined through Cronbach's alpha coefficient test. *Table 2* 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 |
|---|---|
| IV1: What is the significant relationship between financial literacy on combating the threat of cybercrime | 0.78 |

| | |
|---|---|
| IV2: What is the significant relationship between public awareness on combating the threat of cybercrime | 0.82 |
| IV3: What is the significant relationship between ICT and technical tools on combating the threat of cybercrime | 0.83 |
| IV4: What is the significant relationship between education on combating the threat of cybercrime | 0.84 |
| IV5: What is the significant relationship between law enforcement on combating the threat of cybercrime | 0.86 |
| DV: What is the relationship between all independent variables on combating the threat of cybercrime | 0.77 |

The result in *Table 2* show 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. As Nunnally and Bernstein (1994) who stated that one should strive for 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 (INHAC, 2016).

**4.2. Descriptive Analysis**: **Respondents Profile**

*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 | | |
| | Do not know | 3 | 2.4 | 123 | 100 |

| | | | |
|---|---|---|---|
| Experience in Cybercrime | Never | 23 | 18.5 |
| | Occasionally | 42 | 33.9 |
| | Often | 55 | 45.2 |

Source : Research Findings (2024)

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 experienced or involved 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.

### 4.3. The Multi-collinearity Test

Based on the results of Multi-collinearity test with SPSS Location Statistics for MAC version 24, refers to the value of *Tolerance* than VIF.

*Table 4: Multi-collinearity Test (Coefficient)*

| Model | Collinearity Statistics | |
|---|---|---|
| | Tolerance | VIF |
| *(Constant)* | | |
| The financial literacy have a significant relationship to combating the threat of cybercrime in banking system | .467 | 2.141 |
| The public awareness have a significant relationship to combating the threat of cybercrime in banking system | .454 | 2.201 |
| The ICT and technical tools have a significant relationship to combating the threat of cybercrime in banking system | .567 | 1.765 |
| The education have a significant relationship to combating the threat of cybercrime in banking system | .475 | 2.106 |
| The law enforcement have a significant relationship to combating the threat of cybercrime in banking system | .555 | 2.014 |

*Table 4* that refers to the four independent variables that were examined, found that all a value Tolerance and VIF is between 0.1 and 10.0 then there is no Multi-collinearity problem for each of the independent variables.

### 4.4. Correlation Analysis

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 5: Correlation Coefficient*

| | | **IV 1** | **IV 2** | **IV 3** | **IV 4** | **IV 5** |
|---|---|---|---|---|---|---|
| **DV 1** | Pearson Correlation | .373** | .348** | .402** | .313** | .467** |
| | Sig. (2-tailed) | <.001 | <.001 | <.001 | <.001 | <.001 |
| | N | 123 | 123 | 123 | 123 | 123 |

**. Correlation is significant at the 0.01 level (2-tailed).

*Note:*
*DV1 - Combating the threat of cybercrime*
*IV1 - Financial Literacy*
*IV2 - Public Awareness*
*IV3 - ICT and Technology Tools*
*IV4 - Education Ecosystem / Training*
*IV5 - Law Enforcement*

Based on *Table 5*, 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 under Chapter 1.Based on the table 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, Public Awareness, ICT Tools, Law Enforcement and Education/Training with the relationship in combating the threat of cybercrime are indicated as 0.373, 0.348, 0.402, 0.313 and 0.467 respectively 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.

### 4.5 Multiple Regression Analysis

*Table 6: Multiple Regression Analysis*

| Model | Unstand -ardized Coefficients | Coefficient Std. Error | Standardize d Coefficient Beta | t. | Sig. |
|---|---|---|---|---|---|
| (Constant) | 3.008 | .308 | | 9.778 | <.001 |
| Financial Literacy | .147 | .089 | .233 | 1.643 | .103 |
| Public Awareness | -.128 | .116 | -.185 | -1.103 | .272 |

| | | | | | |
|---|---|---|---|---|---|
| ICT Tools | .080 | .104 | .111 | .773 | .441 |
| Education/Training | -.019 | .092 | -.023 | -.206 | .837 |
| Law Enforcement | .293 | .103 | .388 | 2.844 | .005 |

Multiple regressions here was being calculated and analyzed by the researcher to understand which variables has given the most influence in this study. From here, the researcher will identify which variables that significantly contributes to the core of the study.

*Table 6* above spelled out the relationship between all 5 independent variables and its' significance value (Sig.). Financial literacy, ICT Tools and Law Enforcement have shown marginal value of Unstandardized Coefficient B with 0.147, 0.080 and 0.293 respectively. Unlike Public Awareness and Education/Training which recorded a value of -0.128 and -0.019 respectively. These proven the higher effectiveness of each IVs, the lower exposure of DV into risk of cybercrime.

Moreover, the coefficients of determinant or variance ($R^2$) were also well portrayed in multiple regressions that show how much the IVs are influencing the DV. Likewise, the beta coefficient (β) will describe how much the influence of each IV towards DV. The largest amount of beta value will indicate the strongest contribution on the DV, in absolute value. Similarly, the smaller the beta value will indicate the lesser contributions of IVs towards DV. On top of that, Sig. value (*p*-value) will indicate the significant effect of the IVs towards DV and it should be recorded at less than 0.05 (<0.05) for the significant value of the variables to be guaranteed. (Sekaran and Bougie, 2016).

### 4.6. Model Summary

*Table 7: Model Summary*

| R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|
| .491[a] | .241 | .209 | .35712 |

a. Predictors: (Constant), AVG IV5, AVG IV1, AVG IV4, AVG IV3, AVG IV2
b. Dependent Variable: AVG DV1

Based on the *Table 7,* Model Summary portrayed the value of R, $R^2$, and adjusted R square ($R^2$) as well as standard error of the estimate. This model summary was done by using Enter Method. Based on the table above, the $R^2$ is equivalent to 0.491 = 49.1%, which means that the IV studied in this study is 49.1% representing the DV of the study. Additionally, another 50.9% were explained by other factors. From here, the researcher able to indicate that the IVs studied is relevant to be tested with this DV.

**Table 8: ANOVA**

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Regression | 4.744 | 5 | .949 | 7.440 | <.001[b] |
| Residual | 14.921 | 117 | .128 | | |
| Total | 19.666 | 122 | | | |

a. Dependent Variable: AVG DV1
b. Predictors: (Constant), AVG IV5, AVG IV1, AVG IV4, AVG IV3, AVG IV2

Based on *Table 8* ANOVA as above, it illustrates the Model 1, F-statistics of 7.440 and at significant level of <0.001. (Sekaran and Bougie, 2016) had stated that the model is contemplate significant (*p*-value) when it is less than 0.05 (<0.05). Thus, it shall be extrapolated that the model is significant and acceptable as the *p*-value is less than 0.05 (<0.05). In other words, the researcher manages to obtain all IVs are significant towards the DV as the *p*-value is less than 0.05 (<0.05).

## 5.0. CONCLUSION

### 5.1.1. Hypotheses Testing Summary

The research finding show some hypotheses analysis in this research such as:

*Table 9: Hypotheses Testing Summary*

| Variable | Hypothesis | Results |
|---|---|---|
| Financial Literacy | The financial literacy have a significant relationship to combating the threat of cybercrime in banking system | Accepted |
| Public Awareness | The public awareness have a significant relationship to combating the threat of cybercrime in banking system | Accepted |
| ICT Tools | The ICT and technical tools have a significant relationship to combating the threat of cybercrime in banking system | Accepted |
| Education/Training | The education have a significant relationship to combating the threat of cybercrime in banking system | Accepted |
| Law Enforcement | The law enforcement have a significant relationship to combating the threat of cybercrime in banking system | Accepted |

**Hypothesis Analysis**

Under hypothesis analysis, the researcher shall under all the Research Objectives which has been mentioned previous as per the following;

### 4.7. Hypothesis 1 (Financial Literacy)

The first IV of Financial Literacy has been stated through hypothesis in this study in order 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 significant influence towards the DV. Therefore, the hypothesis of H1 is accepted and the H0 is rejected.

i. **Hypothesis 2 (Public Awareness)**

The second IV of Public Awareness has been stated through hypothesis in this study in order 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 significant influence towards the DV. Therefore, the hypothesis of H2 is accepted and H0 is rejected.

ii. **Hypothesis 3 (ICT Tools)**

The third IV of ICT Tools has been stated through hypothesis in this study in order 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 0.402 at significant value of <0.001. Not only that, the model summary as well as ANOVA also indicated that this IV has significant influence towards the DV. Therefore, the hypothesis of H3 is accepted and H0 is rejected.

iii. **Hypothesis 4 (Education/Training)**

The fourth of ICT Education/Training has been stated through hypothesis in this study in order 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 0.313 at significant value of <0.001. Not only that, the model summary as well as ANOVA also indicated that this IV has significant influence towards the DV. Therefore, the hypothesis of H4 is accepted and H0 is rejected.

iv. **Hypothesis 5 (Law Enforcement)**

The fifth of Law Enforcement has been stated through hypothesis in this study in order 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 0.467 at significant value of <0.001. Not only that, the model summary as well as ANOVA also indicated that this IV has significant influence towards the DV. Therefore, the hypothesis of H5 is accepted and H0 is rejected.

v. **Hypothesis 6 (Mediating – Effectiveness)**

The result shows the effectiveness moderated to strengthen the relationship between all independent variable and dependent variables.

*Table 9 above sh*ows that Summary of Hypotheses all the IVs which has been tested their significant level towards DV. Based on the output by SPSS, the researcher may conclude that all of the 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.

## 5.1 DISCUSSION & RECOMMENDATIONS

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. Some of them here are discussed below:

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 menace. 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 Programmes should be initiated in order 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.

## 5.2 RECOMMENDATIONS TO THE STUDY

### 5.2.1 **How can we protect ourselves against cybercrime.**

Since everyone is vulnerable to the threats of cybercrime, there are simple but proactive steps to avoid becoming victims of cybercrime such as:

i. Never give out personal data over the phone or via email unless you are completely sure the line or email is secure.
ii. Do not open an attachment from a sender you do not know.
iii. Do not click or download any links in spam emails or other messages from unidentified sources.
iv. Check the authenticity of the organizations involved by calling the companies using the number on their official website.
v. Use strong passwords that people will not guess and do not record them anywhere.
vi. Ensure that your antivirus software and operating system are up to date to protect your devices from the latest security threats.

AI is but one of the many aspects that organizations need to incorporate or adhere to in order to maintain a robust cybersecurity posture. For a cybersecurity practice to be successful, organizations need to consider People, Process and Technology, and how each of these contributes to the overall security posture of the organization. To help organizations better withstand and respond to cyberattacks and malware infections, here are five best practices that they can consider in improving their defense against cybersecurity threats:

a. **Position cybersecurity as a digital transformation enabler**

Disconnect between cybersecurity practices and digital transformation effort creates a lot of frustration for the employees. Cybersecurity is a requirement for digital transformation to guide and keep the company safe through its journey. Conversely, digital transformation presents an opportunity for cybersecurity practices to abandon aging practices to embrace new methods of addressing today's risks.

b. **Continue to invest in strengthening your security fundamentals**

Over 90% of cyber incidents can be averted by maintaining the most basic best practices. Maintaining strong passwords, conditional use of multi-factor authentication against suspicious authentications, keeping device operating systems, software and anti-malware protection up-to-date and genuine can rapidly raise the bar against cyberattacks. This should include not just tool-sets but also training and policies to support a stronger fundamental;

c. **Maximize skills and tools by leveraging integrated best-of-suite tools.**

The best tools are useless in the hands of the amateur. Reduce the number of tools and the complexity of your security operations to allow your operators to hone their proficiency with the available tools. Prioritizing best-of-suite tools is a great way to maximize your risk coverage without the risk of introducing too many tools and complexity to the environment. This is especially true if tools within the suite are well-integrated to take advantage of their counterparts.

d. **Assessment, review and continuous compliance**

The organization should be in a continuous state of compliance. Assessments and reviews should be conducted regularly to test for potential gaps that may occur as the organization is rapidly transforming and address these gaps. The board should keep tab on not just compliance to industry regulations but also how the organization is progressing against security best practices.

e. **Leverage AI and automation to increase capabilities and capacity**

With security capabilities in short supply, organizations need to look to automation and AI to improve the capabilities and capacity of their security operations. Current advancements in AI has shown a lot of promise, not just in raising detections that would otherwise be missed but also in reasoning over how the various data signals should be interpreted with recommended actions. Such systems have seen great success in cloud implementations where huge volumes of data can be processed rapidly. Ultimately, leveraging automation and AI can free up cybersecurity talents to focus on higher-level activities.

## 5.3 RECOMMENDATIONS TO THE FUTURE RESEARCHERS

Lesson learnt for future researchers, 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. 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. Furthermore, the google form of questionnaires should also be extended to all commercials banks in other states in Peninsular Malaysia, Sabah and Sarawak.

On the other hand, a future researcher should also completely run the pilot test of questionnaires into IBM SPSS to evaluate the correctness of the questions format, the accurate output of the research so that the research will successfully met and answered the Research Problem.

## REFERENCES

[1] Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47-88.
[2] Baker, P., & Glasser, S. (2005). *Kremlin rising: Vladimir Putin's Russia and the end of revolution*. Simon and Schuster.
[3] Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment*. Sage publications
[4] 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.
[5] Check, J., & Schutt, R. K. (2012). Teacher research and action research. *Research methods in education*, 255-271.
[6] Collins, N. L., & Miller, L. C. (1994). Self-disclosure and liking: a meta-analytic review. *Psychological bulletin*, *116*(3), 457.
[7] Connelly, L. M. (2008). Pilot studies. *Medsurg Nursing*, *17*(6), 411.
[8] Dzomira, S. (2016). Espousal of combined assurance model in South Africa's public sector. *Public and Municipal Finance*, *5*(4), 23-30.
[9] Farhana, S. (2020, October 25). The rise of cybercrime in Malaysia - what you need to avoid. *Astro AWANI*.
[10] Felson, M., & Cohen, L. E. (2017). Human ecology and crime: A routine activity approach. In *Crime Opportunity Theories* (pp. 73-90). Routledge.
[11] Gnaneswaran, D. (2018, July 12). Cybersecurity threats to cost organizations in Malaysia US$12.2 billion in economic losses. *Microsoft Malaysia*.
[12] Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press
[13] Gupta, S. (2012). Buffer overflow attack. *IOSR Journal of Computer Engineering*, *1*(1), 10-23.
[14] Hill, R. (1998). *The mathematical theory of plasticity* (Vol. 11). Oxford university press.
[15] Hill, J. B., & Marion, N. E. (2016). *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century: Computer Crimes, Laws, and Policing in the 21st Century*. ABC-CLIO.
[16] 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*. Edit publishers.
[17] Johanson, G. A., & Brooks, G. P. (2010). Initial scale development: sample size for pilot studies. *Educational and psychological measurement*, *70*(3), 394-400.
[18] Khalid, K., Abdullah, H. H., & Kumar M, D. (2012). Get along with quantitative research process. *International Journal of Research in Management*.
[19] Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and psychological measurement*, *30*(3), 607-610.
[20] Kuder, G. F., & Richardson, M. W. (1937). The theory of the estimation of test reliability. *Psychometrika*, *2*(3), 151-160.
[21] Lakomski, G. (2001). Organizational change, leadership and learning: culture as cognitive process. *International Journal of Educational Management*.
[22] Lowry, R. (2014). Concepts and applications of inferential statistics.
[23] Nachmias, D. (1972). Political alienation and political behavior.

[24] 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.

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

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

[27] 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.

[28] 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. In *The 5th International Conference on Financial Criminology (ICFC)*.

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

[30] Schell, B. H., & Martin, C. (2004). *Cybercrime: A reference handbook*. ABC-CLIO.

[31] Singh, J., & Singh, H. (2012). Continuous improvement approach: state-of-art review and future implications. *International Journal of Lean Six Sigma*

[32] Singleton, R. A., & Straits, B. C. (2012). Survey interviewing. *The SAGE handbook of interview research: The complexity of the craft*, 77-98.

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

[34] *Vladimir. G., (2005). International cooperation in fighting cybercrime. [Online]. Available:* Whiteley, A. (2002). Rigour in qualitative.