# An Empirical Study on Cybercrime:

# The Emerging Threat to Banking Sectors in Malaysia

By

Wan Nora Wan Ibrahim

Project Paper Submitted in Partial Fulfilment of the Requirements

for the Degree of Master of Business Administration

Universiti Tun Abdul Razak

June 2021

# DECLARATION

The author hereby declares that this project paper is the original study undertaken by him unless stated otherwise. Due acknowledgement has been given to references quoted in the bibliography. The views and analyses in this study are that of author's, based on the references made; and this does not constitute an invitation to use this study as a technical tool for management purpose.

Wan Nora Wan Ibrahim
26 June 2021

# ACKNOWLEDGEMENT

Firstly, my acknowledgement goes to the Almighty for giving me strength for having come this far. With my tight schedule of work obligation as a banker, wife and a mother to my two children, I am able to cope with the study under post graduate level at UNIRAZAK and subsequently completed my research paper. My deepest gratitude extended to my research supervisor, Assoc. Prof. Dr. Mohd Yaziz Mohd Isa for his excellent guidance, cooperation and supervision in completing this project paper titled **"An Empirical Study on Cybercrime: The Emerging Threat to Banking Sectors in Malaysia"**. I would also like to express my appreciation and many thanks to all the faculty lecturers who have been giving lectures, guidance and assistant during my two years studying under MBA (Majoring in Finance) UNIRAZAK program.

As a mother to my two children, special thanks to my children for giving continuous support to my study, my good friends for giving me encouragement and motivation throughout my two years journey. Not forgotten, all my classmates under Cohort July 2019, we strive a strong spirit together to pursue our goal. We motivate and support each other, sharing knowledge and work in a team to complete a group assignment. I proud of you all. Millions of thanks to the group of experienced and credible lecturers where they have been sweating to pour knowledge regardless of time even during the pandemic COVID-19. The support groups such as the Academic Division, SKC teams for direct and indirect support throughout my study period.

To my both beloved father and mother, I would thank you from the bottom of my heart on your appreciation and acknowledgement on my study.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF DIAGRAMS

## LIST OF FIGURES

Abstract of the Project Paper Submitted to the Senate of Universiti Tun Abdul Razak in Partial Fulfillment of the Requirements for the Master of Business Administration

**An Empirical Study on Cybercrime:**
**The Emerging Threat to Banking Sectors in Malaysia**

**By**
**Wan Nora Wan Ibrahim**

**June 2021**

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. 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. 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. The present study focus on banking sector so it's 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. 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. 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.

# CHAPTER 1
# INTRODUCTION

## 1.1 Background of the Study

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.

### 1.1.1 Terminology

*Table 1: Terminologies the Techniques and Tactics on Cybercrimes*

| No | Terminology | Explanations |
|---|---|---|
| 1. | Identity Theft | • One of the common techniques used by computer hackers when dealing with online businesses, in particular the online banking medium, is the 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. |
| 2. | Phishing | • 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. Suppose that electronic services are rendered by a legal corporation. The AFCC, the Anti-Fraud Main Base, has estimated the total numbers of phishing scams in 2014 that cost $4.5 billion in damages. |
| 3. | Vishing | • 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 |

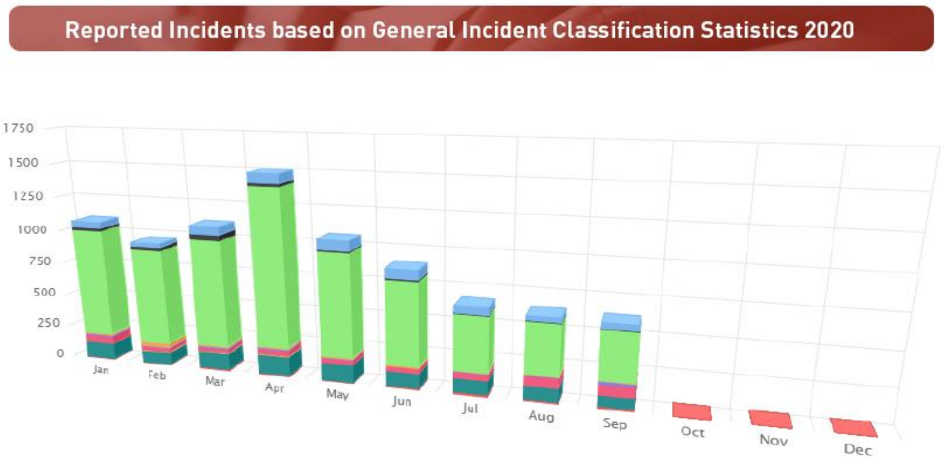
| | | |
|---|---|---|
| | | company/organization. The AFCC, the Anti-Fraud Main Base, has estimated the total numbers of phishing attacks in 2014 that cost $4.5 billion in damages. |
| 4. | Malware | • The most significant vulnerability available to cyber criminals to gain unauthorized access to systems to steal their monetary as well as other confidential data is malware (Viruses, Viruses, Trojans and other threats). The rapid growth of mobile devices such as cars and tablets is 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.<br>• The rapid growth of mobile items, for examples smartphones and tablet personal computers, contributes to high potential of malicious malware apps. In recent years, computer fraudsters have been using malware programs to commit one hundred thousand of frauds against online customers in the business sector. In particular, online banking, with the intention of extracting large amounts of money. As the rising smartphone medium, including such android, mobile phones are important to note, which is perhaps the most attacked stage by malware writers and that there is a growing need to create robust protections against them. |
| 5. | Automating Online Banking Fraud | • With the aid of Automatic Transfer Systems, cyber criminals and computer fraudsters have now taken it a step further (ATSs). A new method for Automating Online Banking Fraud has been started using malware variants in combination with Spy Eye and Zeu S. A text file with a lot of JavaScript and HTML codes is a part of |

|  |  |  |
|---|---|---|
|  |  | web inject files. |
| 6. | Social Engineering | • It is the practice of influencing someone to carry out acts or to divulge sensitive information.  Cyber criminals and computer fraudster has widely used the social science discipline of the social engineering, in collecting financial data and to gain unauthorized an access to secret information. |
| 7. | Social Networks | • For cyber fraudsters, social networks are common platforms to obtain information shared by credit card holders. For illegal purposes, information gained by cyber scammers will later be used. These social media sites, such as Twitter and Facebook, allow users to access an instant message and can revert users to some other was alone with an instant message pop-up during the process. |

### 1.1.2 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.

*Figure1: Reported Incidents based on General Incident Classification Statistics 2020 – MyCERT*



*Source: Ministry of Multimedia and Communication (MCMC) Report*

The above *Figure1* 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 cyber threat respectively.

## 1.2 Problem Statement

The Government of Malaysia as well as Bank Negara Malaysia through all commercial banks in Malaysia has 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;

A. Analyze the relationship between financial literacy on combating the cybercrime, an emerging threat among customers in banking sectors of Malaysia

B. To investigate the relationship between public awareness in combating the threat of cybercrime in banking sectors.

C. 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.

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

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

## 1.4 Research Questions

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

A. What is the relationship between the factors of financial literacy on combating the threat of cybercrime in banking sectors?

B. What is the actual situation on the public awareness on cybercrime an emerging among customers banking sectors in Malaysia?

C. What is the relationship between the factor of Information Technology Communication (ICT) tools and Prevention Techniques on combating the threat of cybercrime in banking sectors?

D. What is the relationship between the factors of education ecosystem on combating the threat of cybercrime in banking sectors?

E. What is the relationship between the factors of law enforcement on combating the threat of cybercrime in banking sectors?

## 1.5. Hypothesis of Research

In line with the main of research objectives and questions stated the following of specific research hypothesis;

A. H1: Is there the significant relationship between the factors of financial literacy on combating the threat of cybercrime in banking sectors.

B. H2: Is there the significant relationship between the factors of public awareness on combating the threat of cybercrime in banking sectors.

C. H3: Is there the significant relationship between the factor of Information Technology Communication (ICT) tools and Prevention Techniques on combating the threat of cybercrime in banking sectors.

D. H4: Is there the significant relationship between the factors of education ecosystem on combating the threat of cybercrime in banking sectors?

E. H5: Is there the significant relationship between the factors of law enforcement on combating the threat of cybercrime in banking sectors?

## 1.6 Significance of the Study

### 1.6.1 To the Study (Researcher)

From the researcher's observation, there are a very limited study or research that involved the modus operandi of cybercrime in Malaysia and methods of combating cybercrime especially in banking sectors in Malaysia. As such, the researcher makes this study to be the eyes opener to the banks employees and management to take priority on the emerging threat of cybercrime. The study is also being conducted to support academic research and the banking institution in Malaysia.

### 1.6.2 To the Banking Industry

In order to thrive and develop in a global competitive scenario, the time has come where it is important to address the security aspects of banks on a priority basis. That said, with the increase in cybercrime cases, proactive measures to counter crime are urgently needed. A global electronic crime for the sophistication of its investigation need a global presence. As a result, the steps taken by banks are inadequate, increasing collaboration between banks around the world is essential for the development of tools and models that can be used to address global cybercrime in banking. The study is vitals especially to banks customers in order to avoid any financial losses and misused of personal data by cyber criminals. It also contributes to prudent banking image and high level of trust by consumers towards banking sectors if the cybercrime is mitigated.

### 1.6.3 To the Policy Maker (Government)

The government of Malaysia should foresee the seriousness in combating the emerging threat of cybercrime. The rising cybercrime wave makes 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 government of Malaysia through an enforcement agency should establish the task force team in order to mitigate any cybercriminals and to provide an expertise for relevant cybercrime cases.

## 1.7 Limitation of study

a. The study was only conducted to the Banking sectors in Malaysia. It could be enhanced into other sectors which also exposed to the risk of cybercrime.

b. The samples selection based on the participating of respondent’s in Google form of questionnaire from 16 April to 07 May 2021 (3 weeks).

c. Only constructs taken as independent’s variables. It could also be considered from other factors.

d. Did not take into considerations the blueprints, policies and strategies to combat the cybercrime from government’s perspectives.

## 1.8 Operational Definition

a. **Financial literacy** - It is important to 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.

b. **Public awareness** – Public to aware on the cybersecurity awareness, including corporate security awareness, security awareness material on the intranet website, information on screensaver and so on.

c. **ICT and technical tools** – In banking sector, ICT and technical tools are the major component and have advantage to give prevention, detection and response. Banking sectors must choose the most reliable and right cyber security solution for the.

d. **Education ecosystem** – All the banks employee must be provided with sufficient education and training on types of cybercrime and strategies in combating the threat of cybercrime in banking sectors.

e. **Law enforcement** – It plays a key role in implementing the cyber security priorities of our nation by examining a wide variety of cybercrimes, including the fraudulent activity in financial transaction, to arrest and imprisonment.

## 1.9 The Organization of the Study

This study is divided into five (5) chapters which are included as follows;

a. **Chapter 1:** Introduction that describes the study background, overview of cybercrime, research of problem statement, research objectives, research questions, hypothesis analysis, significant of study and the organization of the study.

b. **Chapter 2:** Overview of the Literature Review which describes on underpinning theory and theoretical framework, review of the prior empirical studies and proposed the conceptual framework.

c. **Chapter 3:** Overview that illustrates the research methodology, the research design, sampling design, pilot test, data instruments, data analysis, validity and reliability test, structure of questionnaire and types of data analysis.

d. **Chapter4:** Overview that research analysis, research finding, hypothesis testing and structure of research finding presentation.

e. **Chapter 5:** Research summary, conclusion of study, recommendation to the researcher and recommendations to the future researchers.

# CHAPTER 2
# LITERATURE REVIEW

## 2.0 Introduction

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware legal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks. A primary effect of cybercrime is financial; cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may also target an individual's private information, as well as corporate data for theft and resale. As many workers settle into remote work routines due to the pandemic, cybercrimes are expected to grow in frequency in 2021, making it especially important to protect backup data.

## 2.1 A Related Studies on the Online Banking Cybercrime

In measuring the online banking customers' behavior, Ali, L., Ali, F., Surendran, P., & Thomas, B (2017) from their International Journal of e-Education, e-Business, e-Management and e-Learning titled the effects of cyber threat on customer's behavior in e-Banking services has spelled out the behavior of over 100 users of online banking and assessed the effect on these users of cyberattacks. This study survey included a total of 110 banking customers and three high schools. The data was collected from banking customers aged 18 years and above.

*Diagram 1: Frequency of Online Banking Services by Online Customer*

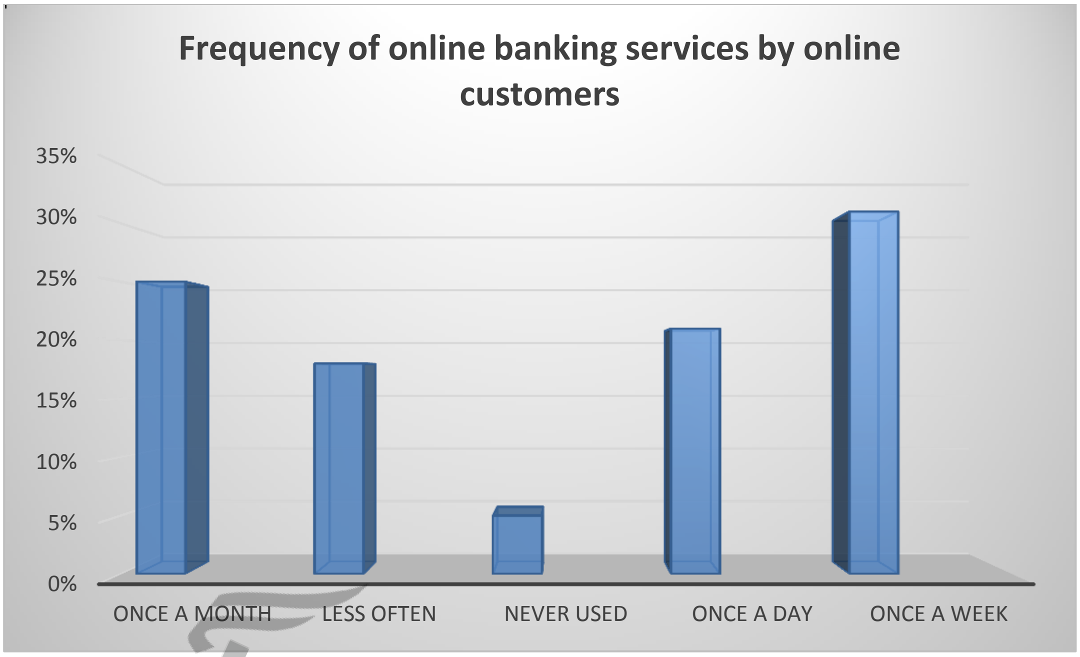


*Diagram 1* reveals clearly indicates that only 21% of users of the online banking facility each day and 31 per cent use online banking facility once a week. The study indicates that participants do online banking, with the exception of 5%. 25% of respondents indicated that they use the online banking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

*Diagram 2: Types of Threats*

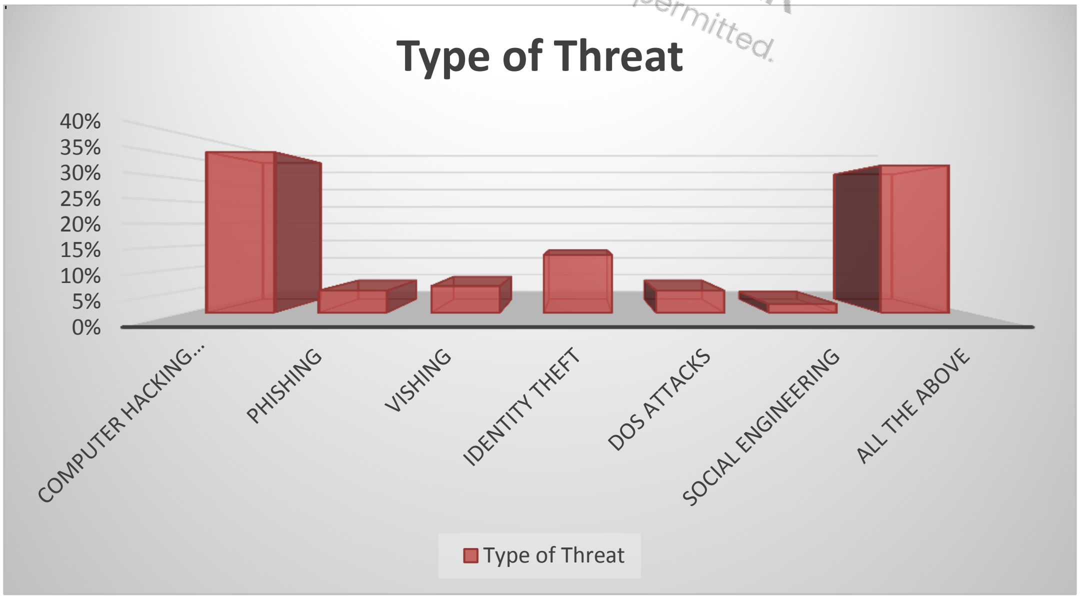
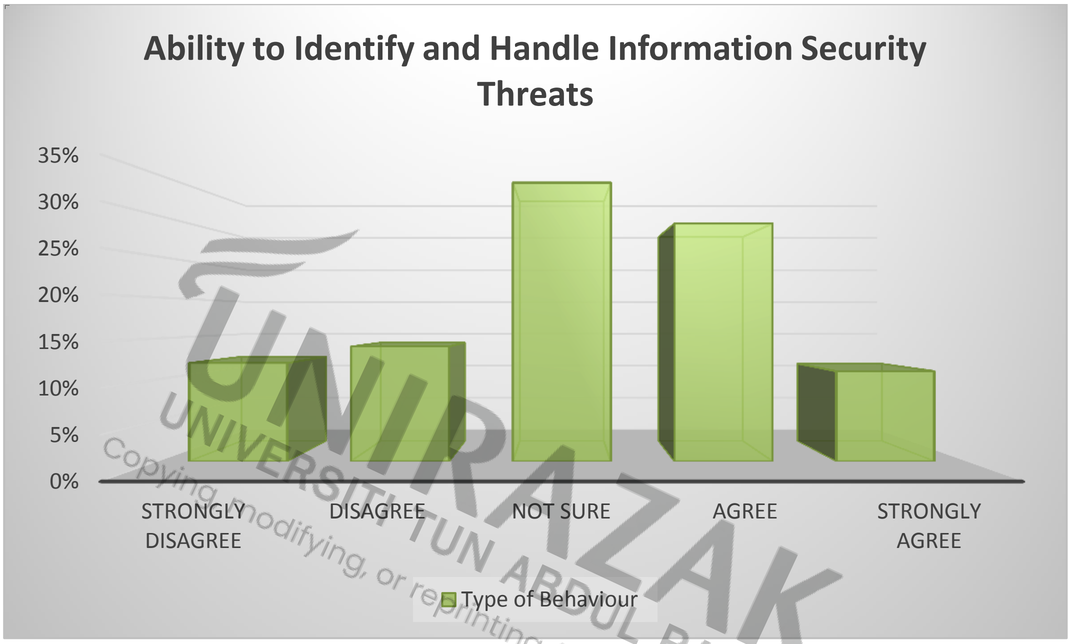


Diagram 2 shows the level of knowledge among respondents about online banking facility and potential of cyber-criminal.  As provided, 37% of respondents were aware of computer hacking, 6 percent were aware of phishing, while another 6 percent reported that they were aware of hacking (phishing over VOIP).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

*Diagram 3:  Ability to Identify and Handle Information Security Threats*



*Source:  International Journal of e-Education, e-Business, e-Management and E-Learning, 7(1), 70-80.*

An analysis of the said Diagram 8 indicated that only 40% of respondents were can identify information of security criminals and able to deal with such criminals.  On the other hand, 35% of respondents to the survey are in doubt in managing the available threats. According to the above analysis, 26% of respondents are unable to identify such threats and are also unable to deal with such threats.

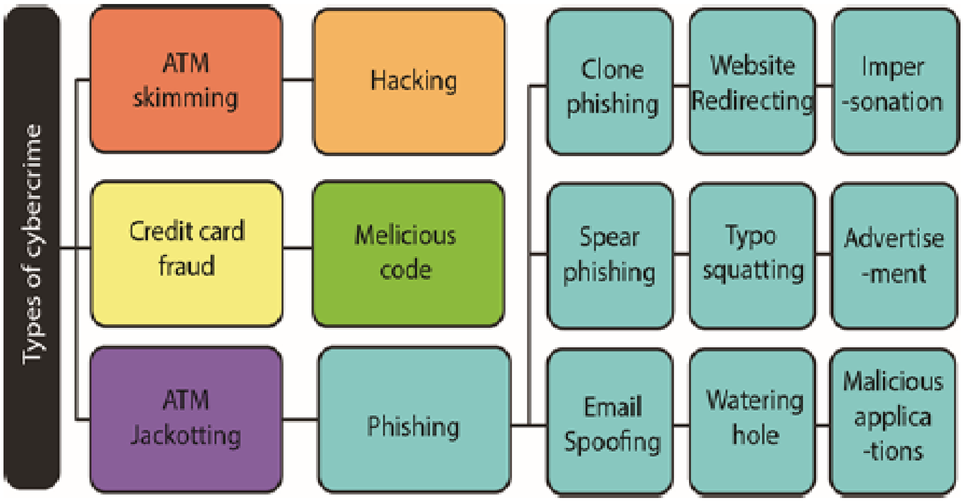
## 2.2 Empirical Studies of Cybercrime from Others Researchers

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 matterby 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 4: Type of cybercrimes in banking sector*



Based on 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 frontliner as 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.

# LITERATURE REVIEW

## 2.3 Literature review

| Bil | Nama | Year | Title | Research Finding |
|---|---|---|---|---|
| 1. | EdySantoso | 2012 | Consumer Protection for online banking Scams via e-mail in Malaysia | The new advancement in technology both hard and soft is creating new opportunities for cyber criminals. 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. Therefore, the objectives of this paper are to identify cyber scams via email in online banking business model and to examine consumer protection of online banking scams in Malaysia. |
| 2. | MaslinaDaud et.al., | 2018 | Bridging the gap between organizational practices and cyber security compliance: Can cooperation promote compliance in organizations? | Drawing on public goods and institutional theory, this study examines the mediation effect of cooperation 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. Using data from |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  |  | Malaysia’s critical sectors, ordinal regression was used to establish the odds of security compliance with security practices adjusted for job portfolio, security responsibility and educational levels. The 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. |
| 3. | Shanit Khan et.al., | 2018 | Cybercrimes: A Growing Threat to India Banking Sector | With the advancements in technology, the Indian Banking Sector has been at par with the emerging trends and significant changes required in its operations. 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 a period of 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 the major motivation behind most cybercriminal activities and there is little chance of this changing in the near future. 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. |
| 4. | Siyanda Dlamini et.al., | 2019 | Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses | Cybercrime continues to be a detrimental problem in South Africa and continues to change in nature and sophistication. 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. The policing of cybercrime is generally an afterthought for several organizations and individuals in South Africa. This type of crime has no regional, national or international boundaries, unlike “traditional crime” which has physical boundaries and limits in relation to |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  |  | jurisdiction. This contributes towards the challenge of detecting, investigating and combating it. Cyber criminals have intercepted vital and essential government, personal and business information online. Therefore, the primary objective of this paper is to explore the obstacles/challenges that hamper the effective and efficient policing of cybercrime in Durban, South Africa. A qualitative research approach was adopted, to explore the challenges of policing of cybercrime in the study area. The findings collected through semi-structured interviews with a total number of twenty (20) participants comprising of SAPS Directorate for Priority Crime Investigation (DPCI) officials, members of Bowline Security and members of the Durban community; suggest that there is a shortage of SAPS officials who are knowledgeable in handling cybercrime related cases. Policies and strategies to police cybercrime in Durban are insufficient because of the lack of resources, to adequately implement policy and promote cooperative strategic partnerships. Together, these findings suggest that all relevant stakeholder organizations should assist in minimizing the challenge of policing of cybercrime. |
| 5. | Ajeet Singh Poonia | 2014 | Cyber Crime: Challenges and its Classification | Digital technology is encompassing in all walks of life, all over the world and has brought the real meaning of globalization. At the one end cyber system provides opportunities to |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  |  | communicate and at the other end some individuals or community exploit its power for criminal purposes. Criminals exploit the Internet and other network communications which are international in scope. Situation is alarming; Cybercrime is an upcoming and is talk of the town in every field of the society/system. Theoretically and practically, this is a new subject for researchers and is growing exponentially .Lot of work has been done and endless has to be go because the invention or up gradation of new technology leads to the technical crime i.e. the digital or we can say the cybercrime or e-crime. This is because every day a new technique is being developed for doing the cybercrime and many times, we are not having the proper investigating method/model/technique to tackle that newly cybercrime. |

## 2.4 Theoretical Underpinning Literature Review of Theories

There are five (5) theories have been identified and related to the study;

### A. Social Learning Theory

It 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, Albert (1963). This process is referred to as vicarious strengthening. Kids and adults often display learning stuff as an example of this theory, even though they have no direct experience of it. They can learn new information or follow others behavior or doing things by observing others doing so.

### B. The Low Self-Control Theory of Crime

This is the most criminological theories of recent decades as developed by the criminologists Gottfredsonmand Hirschi (1990). 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 Muraven, 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. An example under this theory is when people are in constraint situation involving financial tight financial commitment, they tend to do the illegal actions in order to gain the money. The action will finally cause the financial loss of the victim and legal actions will be taken on the criminal offences.

### C. General Strain Theory (GST)

According to Agnew (1992), he was the one who developed this theory. The hypothesis has received a considerable amount of attention by academician since it was established. It states that 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. Agnew (1992) recognized that in terms of fully constructing the variety of available sources of strain in society, particularly among the younger generation, the conflict perspective originally put forth with Robert King Merton was limited. Innovation occurs, according to Chen (2014), when culture pressures socially beneficial and agreed targets. While providing an inadequate opportunity to achieve this goal at the same time.

In other worlds, to achieve socially acceptable goals, those members of society who are in a position of financial strain and still want to attain material prosperity must turn to crime. Agnew (1992) supports this belief and acknowledges that there are other variables that encourage illegal activity in dealing with young people. He reveals that not only people facing financially induced, but the inadequate experiences can also contribute to stress and subsequently involve in criminal offences.

### D. Routine Activity Theory

This theory is a sub-field of the theory of opportunities for crime that focuses on crime situations. In their explanation of the changes in the crime rate in the United States among both 1947 and 1974 (Felson & Cohen, 2017). It underlines, thus according to Cohen and Felson (1979), that when the three (3) components converge, crime occurs. The first is a taking action with knowledge of the attack and the capacity to operate on these inclinations, the second is an appropriate victim or target, and the third is the lack of a capable guardian who can prevent this same crime from occurring. This theory also includes the routine activities of both offender and the victim. An example of this theory is in the case of CCTV in the banking hall of the bank. Normally the CCTV will focus on the critical area imposed to the situation dealing with customers' transactions. If the CCTV is loss of direction of focus and or not in good working condition, such as poor focus image, this situation can lead to fraud case. The fraudster cannot be identified clearly and the routine activity theory looks at crime from an offender's point of view.

### E. Situational Crime Prevention Theory (SCP)

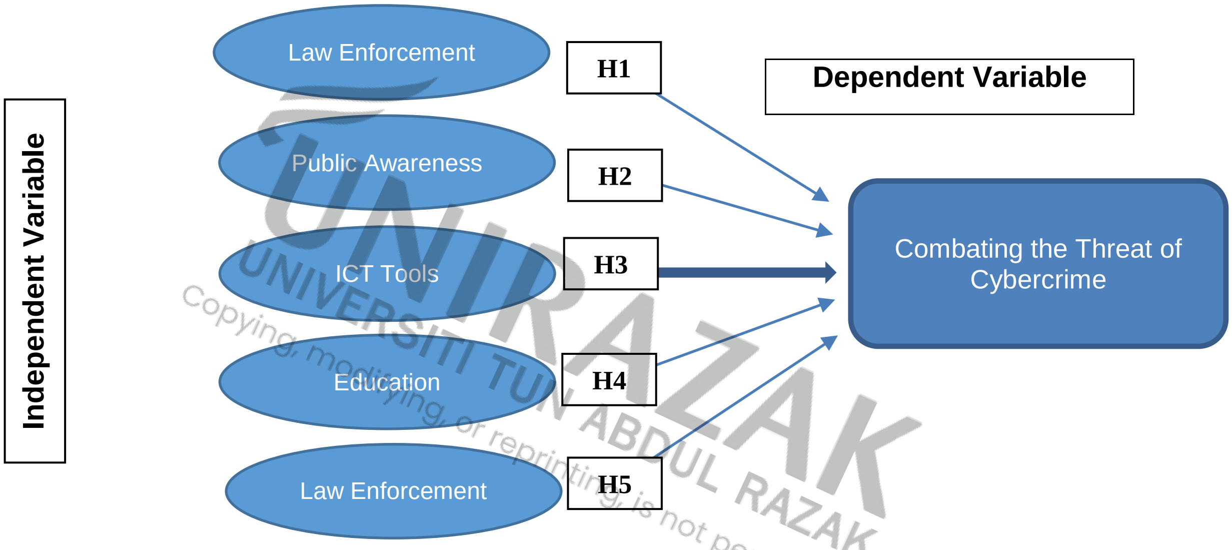
This philosophy focuses on the setting of criminal acts rather than on the nature of the perpetrator. Offenders tend to commit crime on the basis of their understanding of the opportunities available. As a consequence, the situational factors can promote crime, and they can mitigate crime. By altering instantaneous or relational environmental conditions where crime occurs regularly, SCP pursues to people who are affected by crime. This measure involve the environment strategies to increase risk and to reduce crime opportunities. An example of the SCP is the installation of surveillance equipment such as public phone, public toilet in areas that experience a lot of vandalism. Another example could be the installation of security screens in the banks for prevention of robberies. The rising numbers of empiric and experimental research have shown the efficacy of SCP in reduction of crime. The SCP strategy ultimately leads to change in responsibility for the prevention and to minimize the crime away from the police and to other agencies, both public and private sectors.

In the study, the researcher has been emphasizing the Self Learning Theory as it is a learning process and new information behavioral that attains by observing and replying of questionnaires on the suggested variables. Besides that, the researcher has also exercising General Strain Theory (GST) as the study states that strains increase the probability of crime which is seen unfair associated by low social control, creating pressure and rewards for criminal coping. Another theory used by the researcher is Situational Crime Prevention Theory (SCP) which focuses on enforcement of the cybersecurity act by increasing risk and subsequently to reduce the crime opportunities.

## 2.5 The Theoretical Framework

The proposed of theoretical framework in this study which include the 5 independent variables and one dependent variable that show in diagram 6 below:

*Diagram 5: Proposed Theoretical 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

## 2.6 Operational Definition of Variables

### 2.6.1 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;

**a. 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 you.

- 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.

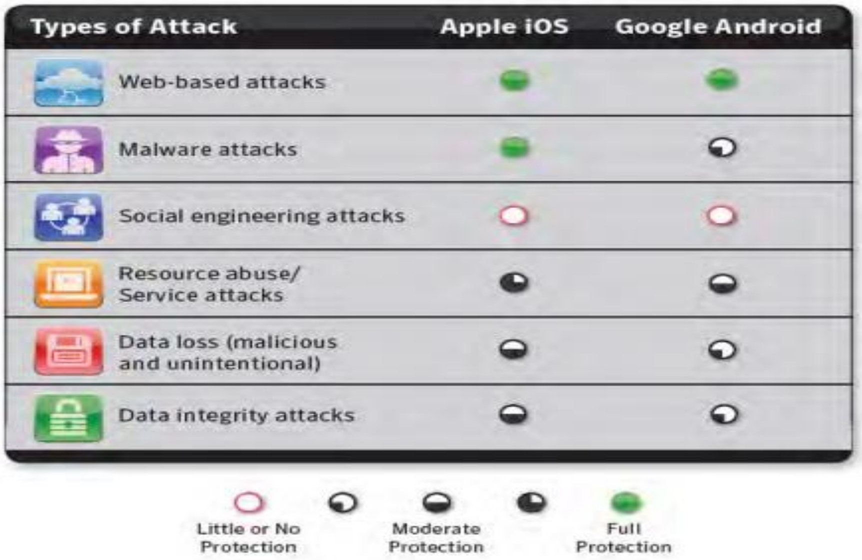
### b. Public Awareness

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.

### c. Information Communication Technology (ICT)

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 6:  Mobile Platform Security Summary*



| Types of Attack | Apple iOS | Google Android |
|---|---|---|
| Web-based attacks | 🟢 | 🟢 |
| Malware attacks | 🟢 | ◔ |
| Social engineering attacks | ○ | ○ |
| Resource abuse/ Service attacks | ◕ | ◑ |
| Data loss (malicious and unintentional) | ◑ | ◔ |
| Data integrity attacks | ◑ | ◔ |

○ Little or No Protection ◔ ◑ Moderate Protection ◕ 🟢 Full Protection

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 machine 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.

### d. 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 work life.

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.

### e. 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.

### 2.6.2 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.

### a. Combating the Financial Threat in Banking Sectors

This is a manipulated variable that are preprogrammed before the first analysis is started. In experimental tests, they were mostly carefully monitored or assigned in controlled experiments. 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 known as 'Combating the financial threat in banking sectors'.

The five independent variables have been drawn on the left of the framework, followed by respective hypothesis which act as a bridge to the effectiveness. The effectiveness of the research methods is identified from research survey on the target sample size and population drawn in the study. Each of the components has an essential role. According to Miles as well as Huberman (1994), the biggest differentiators, constructs, relevant factors and the presumptive relationship between them are laid out in a conceptual framework. The concept statement is a set of goals and basics that are interrelated. The objective is to clearly define the objectives and purpose of the study, and the fundamental principles are the endeavor that help to achieve the goals.

## 2.7 Hypothesis Analysis and Development

The hypothesis is the specialized predictions of what in a particular study will happen. It is developed by using rationale to infer what occurs in the particular circumstance of interest by assessing the existing evidence. It is also generated from the theories associated with it. Hypothesis Expansion is the connection between each of the variables used in this research to produce the outcome of the dependent variable. A study hypothesis is a specific, clear and testable statement or control measure about the possible outcome of the study based on a specific population property, such as the assumed difference between the two groups and a specific variable or interaction between variables. Based on the element of constructs provided in item Proposed Conceptual Framework, the following hypothesis are developed in alternative hypothesis H form;

H1: Is there a significant relationship between financial literacy by banks' customers related to the threat mitigation.

H2: Is there a significant relationship between the public awareness programs related to the threat mitigation.

H3: Is there a significant relationship between that Information Communication Technology (ICT) tools and prevention techniques relate to threat mitigation.

H4: Is there a significant relationship between the educations ecosystem for banks' employees help to mitigate the cyber threat.

H5: Is there a significant relationship between the law enforcement plans relates to mitigate threats.

Those hypotheses will be surveyed to the targeted populations and samples to proof the effectiveness and acceptance of the constructs. Should the respective hypothesis are positive and accepted, its mean the proposed constructs are genuine and suitable for the objective of mitigating the cyber threat in banking sectors in Malaysia.

## 2.8 Summary

The most important material mentioned by the investigator in the studies for the research area has been presented in this chapter. Computer crimes theories can provide perception of the threat's nature, characteristics and acts and victims. A theoretical and conceptual framework has been developed for identification of economic foundations for attack, corporate governance practices, the type of cybercrime in banking, and aspects of its detection and prevention.

The body of empirical evidence for hazard in the banking sector has been reviewed by providing detailed knowledge and evidence on areas concern, such as the use of auditing practices. It is proven from the literature review the most of the analysis and studies on threat mitigation has been carried out in every countries in the world such as Great Britain, Australia and United States. A strong case of cyber threat has been presented in research in Africa. In the Chapter 3, the study will cover the research methodology.

# CHAPTER 3
# RESEARCH METHODOLOGY

## 3.0 Introduction

The research methodology highlights the various methods that will be considered in conducting the research. The research philosophy and the actual considerations which relevant to the research. The topic discussed with the identifying various types of cybercrime, impact on the financial threat to the banks' customers as well as the banking sectors and strategies to combat the cyber threat in banking sectors in Malaysia. A qualitative survey is a primary descriptive will be discussed and explore in nature, beside the quantitative which also be considered.

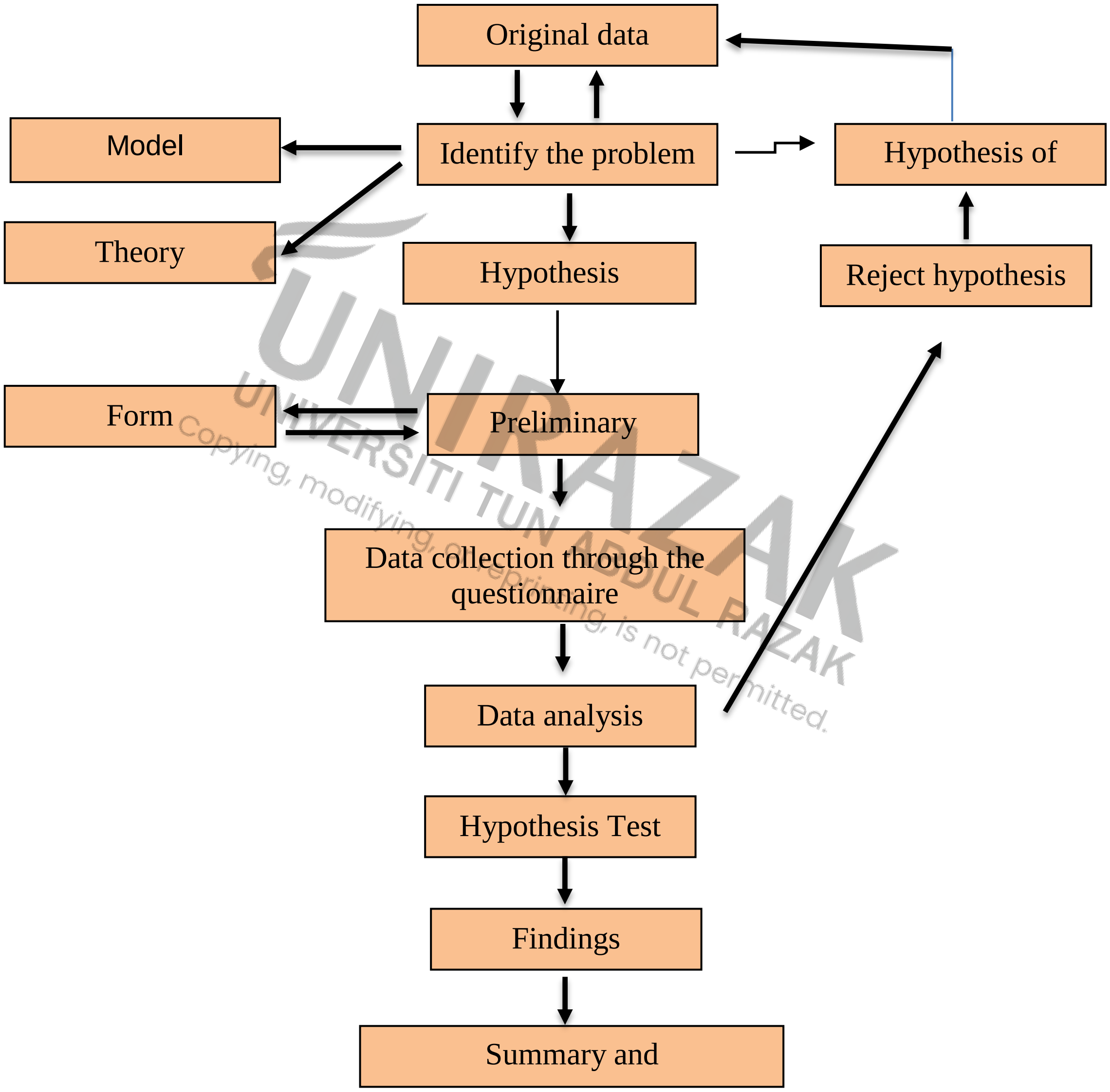
This chapter addresses an approach and the methods to be used in the model of this report. The triangular study model incorporating the quantitative and qualitative approaches of the questions and the surveys with a view in analyzing the survey issues is adopted. The chapter also addresses a different techniques of the research methodology, which includes the research model, population and sampling procedures, data collection methods, operationalization and measurement and data analysis techniques.

## 3.1 Research Design

The research design is the "blueprint" that enables the investigator to come up with solutions to the problems and guides the researcher in the various stages of the research. The purpose of using the research design is to describe the processes involved in designing a study and to demonstrate how the specific research design that a scientist decides to use helps to structure the collection, analysis, and interpretation of data (Nachmias, 1972).

The design study established a set of issues/phenomena that lead to systematic research. If the problem is identified, the goals/objectives of the research in the further research will be advanced. Next, the further discussion will be on the scope, the significant and the limitations of the study, determined to facilitate the process, carried out as in Diagram *9.* At this stage, a population and sampling technique is defined, and human constructions that create links with professionals and ethical behavior are identified. The models, sampling techniques, cross-study and number of samples were then determined.

*Diagram 7: Processes in Research Design Studies*



In the selection of the examination study, researchers elect several respondents exposed to a population of sporadic. The selection of samples to be taken covers of the objective a) the Study; b) To identify the necessary sources of information; c) The identification of the target audience; d) Determination of the sample size taken; e) Define survey; f) Ensuring collection of instrument and data; g) Define the statistical data and hypotheses and h) Testing methods. It all would be general conclusions, summary and recommendations for the study.

In this study, the humanitarian element of cultural academic quality is limited. This includes spirituality, which apply to previous researchers. Studies were then built, and Cross-sectional study done to determine the reliability of every question of the issue built. Once the questionnaires are better is given to everyone, the selected respondents (Banks Employees) as the occasional respondents. Selected respondents are given a specific period that corresponds to each object in the questionnaire. Research design type can be distinguished to four majors:

i. Experimental design, individuals or other units of analysis are randomly assigned to the experimental group. Such design allows for comparison, control, manipulation, usually and generalizability.

ii. Quasi-Experimental design, also in cross sectional designs ordinarily include combinations of some of these elements but not all of them. Typically, these designs lack possibility for manipulation and randomization.

iii. Pre-Experimental design includes even fewer safeguard than quasi-experimental and cross-sectional designs, and in this sense, they provide the least credibility in determining whether two or more variables are causally related.

iv. Cross Sectional design is the most predominant design used in the social sciences. Variables are assayed once and the relationships between them are determined.

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 Study population and Sampling Procedures

The random sampling is use in this method to reduce the sampling error in a particularly small sample size. Random sample were used when difficulties arise such as heavy getting a list of members in a population or not destined to go to any site review. Things like in samples are random people, events and so on. The selected samples represent other samples that arise from the study group randomly, not as an individual.

The sampling techniques used by researchers are the sampling of random. Random sampling is used when the population may divide units in each unit with the characteristics of the population. After a few units are selected randomly, elements of this unit are selected randomly to form a random sample. The study does not take any staff involved in large populations due to limitations on financial resources, intuitive work and a finite time complicates researchers.

## A. 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 are very wide by its look on Malaysian citizen who have experience on the cybercrime cases and adaptive the online banking system. In deed that this study will focusing on the bank clients from state of Pahang who have experience in cybercrime, consisting of clients of banks as well as employees of banks.

## B. Survey

Survey research has historically included large population-based data collection. The primary purpose of this type of survey research was to obtain information describing characteristics of a large sample of individuals of interest relatively quickly. Large census surveys obtaining information reflecting demographic and personal characteristics and consumer feedback surveys are prime examples. These surveys were often provided through the mail and were intended to describe demographic characteristics of individuals or obtain opinions on which to base programs or products for a population or group (www.ncbi.nlm.nih.gov).

Survey research is a useful and legitimate approach to research that has clear benefits in helping to describe and explore variables and constructs of interest. Survey research, like all research, has the potential for a variety of sources of error, but several strategies exist to reduce the potential for error. Advanced practitioners aware of the potential sources of error and strategies to improve survey research can better determine how and whether the conclusions from a survey research study apply to practice (www.ncbi.nlm.nih.gov).

Survey research is used as one of the tools to collect information for this research. Survey research is one of the most important areas of measurement in applied research. The broad area of survey research encompasses any measurement procedure that involves asking questions or respondents. Survey research the process of data collection by distributing the questionnaire to the target population (from 16 April to 07 May 2021) and give them time (3 weeks) to return the questionnaire and obtain the respondent responses. The survey can be used for two main reasons such as to estimate the characteristics of the population and for hypothesis testing (Whiteley, 2002).

Information has been obtained from individuals and groups using survey research for decades. It can range from asking a few targeted questions of individuals on a street corner to obtain information related to behaviors and preferences, to a more rigorous study using multiple valid and reliable instruments. Common examples of less rigorous surveys include marketing or political surveys of consumer patterns and public opinion polls (www.ncbi.nlm.nih.gov).

## C. **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 a random sampling because to ensure that the sample accurately represents the whole population. The target participants for this research is 140 but only 123 respondents (88%) who have experience on cybercrime were randomly selected who are responding by using google form of questionnaires from 16 April 2021 to 07 May 2021 (3 weeks).

Notifying from Rubin and Levin (1998) says that the sampling technique is the methods of collection of some elements of a sample population of reviewed from. A correspondence between the elements of the sample taken from the population, then the better the results obtained. The sample taken must represent the population and can provide an estimate of the value of the Inferential in the population (Lowry, 2014). Generally, the determination of sample size on schedule the determination of sample size studies submitted by cognitive styles on and Krejcie and Morgan (1970) can be used. The number of samples taken is 123 respondents as shown in *Table 2.*

*Table 2:  Schedule of a Study Sample Size Determination*

| Population | Sample | Population | Sample | Population | Sample | Population | Sample |
|---|---|---|---|---|---|---|---|
| 10 | *10* | 150 | 108 | 460 | 210 | 2200 | 327 |
| 15 | 14 | 160 | 113 | 480 | 214 | 2400 | 331 |
| 20 | 19 | 170 | 118 | 500 | 217 | 2600 | 335 |
| 25 | 24 | **180** | **123** | 600 | 226 | 2800 | 338 |
| 30 | 29 | 190 | 127 | 600 | 234 | 3000 | 341 |
| 35 | 32 | 200 | 132 | 650 | 242 | 3500 | 346 |
| 40 | *36* | 210 | 136 | 700 | 248 | 4000 | 351 |
| 45 | 40 | 220 | 140 | 750 | 254 | 4500 | 354 |
| 50 | 44 | 230 | 144 | 800 | 260 | 5000 | 357 |
| 55 | 48 | 240 | 148 | 850 | 265 | 6000 | 361 |
| 60 | 52 | 250 | 152 | 900 | 269 | 7000 | 364 |
| 65 | 56 | 260 | 155 | 950 | 274 | 8000 | 367 |
| 70 | 59 | 270 | 159 | 1000 | 278 | 9000 | 368 |
| 75 | 63 | 280 | 162 | 1100 | 285 | 10000 | 370 |
| 80 | 66 | 290 | 165 | 1200 | 291 | 15000 | 375 |
| 85 | 70 | 300 | 169 | 1300 | 297 | 20000 | 377 |
| 90 | 73 | 320 | 175 | 1400 | 302 | 30000 | 379 |
| 95 | 76 | 340 | 181 | 1500 | 306 | 40000 | 380 |
| 100 | 80 | 360 | 186 | 1600 | 310 | 5000 | 381 |
| 110 | 86 | 380 | 191 | 1700 | 313 | 75000 | 382 |
| 120 | 92 | 400 | 196 | 1800 | 317 | 100000 | 384 |
| 130 | 97 | 420 | 201 | 1900 | 320 | 250000 | 384 |
| 140 | 103 | 440 | 205 | 2000 | 322 | 500000 | 384 |

## 3.3 The Design of a Research Instruments

The Table 2 below describes in detail regarding questions to research, study, hypothesis, data source, data types and techniques of analysis for methodology study, instruments and analysis study

*Table 2: Instruments and Analysis Study*

| Research Question | Research Objective | Research Hypothesis | Source of Data | Data Type | Technique of Analysis |
|---|---|---|---|---|---|
| What is the relationship between the factor of financial literacy on combating the threat of cybercrime in banking sector? | To investigate the relationship between the factor of financial literacy on combating the threat of cybercrime in banking sector. | Is there the significant relationship between the factor of financial literacy on combating the threat of cybercrime in banking sector. | Google form of Questionnaires | Data Primer | Descriptive analysis;<br>• Mean analysis<br>• Pearson Correlation analysis<br>• Cronbach Alpha analysis<br>• Normality analysis<br>• Multiple Regression analysis |
| What is the relationship between the factor of public awareness on combating the threat of cybercrime in banking sector? | To investigate the relationship between the factor of public awareness on combating the threat of cybercrime in banking sector | Is there the significant relationship between the factor of public awareness on combating the threat of cybercrime in banking sector. | Google form of Questionnaires | Data Primer | |
| What is the relationship between the factor of ICT and technical tools on combating the threat of cybercrime in | To investigate the relationship between the factor of ICT & technical tools on combating the threat of cybercrime in banking sector | Is there the significant relationship between the factor of ICT and technical tools on combating the threat of | Google form of Questionnaires | Data Primer | |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| banking sector? |  | cybercrime in banking sector. |  |  |  |
| What is the relationship between the factor of education on combating the threat of cybercrime in banking sector? | To investigate the relationship between the factor of education on combating the threat of cybercrime in banking sector | Is there the significant relationship between the factor of education on combating the threat of cybercrime in banking sector. | Google form of Questionnaires | Data Primer |  |
| What is the relationship between the factor of law enforcement on combating the threat of cybercrime in banking sector? | To investigate the relationship between the factor of law enforcement on combating the threat of cybercrime in banking sector | Is there the significant relationship between the factor of law enforcement on combating the threat of cybercrime in banking sector. | Google form of Questionnaires | Data Primer |  |

## 3.4 Data Collections Method

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.

## 3.5 Process of Data Collection

Questionnaires may be in paper form and mailed to participants, delivered in an electronic format via email or an Internet-based program such as Survey Monkey, or a combination of both, giving the participant the option to choose which method is preferred (Ponto, 2015). Using a combination of methods of google form survey administration can help to ensure better sample coverage (i.e., all individuals in the population having a chance of inclusion in the sample) therefore reducing coverage error (Singleton & Straits, 2012). For example, if a researcher were to only use an Internet-delivered questionnaire, individuals without access to a computer would be excluded from participation. Self-administered mailed, group, or Internet-based questionnaires are relatively low cost and practical for a large sample (Check & Schutt, 2012).

The instrument is a self-administered google form questionnaire which distributed to the participants in the form of questionnaire. In designing the questions in this survey, the researcher using the close-ended question style, the questionnaire (Appendix B) consists of 30 items 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 represented strongly disagrees, 2 represented disagree, 3 neutral, 4 represented agree, and 5 represented 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 (Whitely, 2002). 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 3*, describes and classifies the questionnaires dimensions and number of items for each dimension in Part B.

*Table 3: Questionnaire Dimensions and Number of Items in Section A and B*

| **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* |
| *Questionnaires measuring the relationship between ICT and Technical tools on combating the threat of cybercrime* | *4* |
| *Questionnaires measuring the relationship between education on combating the threat of cybercrime* | *4* |
| *Questionnaires measuring the relationship between law enforcement on combating the threat of cybercrime* | *4* |
| *Questionnaires measuring strategies and solutions for the enhancing the public awareness on cybercrime that an emerging threat to banking sectors in Malaysia.* | *4* |
| ***TOTAL*** | ***30*** |

## 3.6 Research Data Instruments

Each proposal and improvement feedback on each item on the questionnaire derived from this study will be analyzed and used. This is to get the degrees to be high reliability for each of the items on the questionnaire which was built. The instrument was drawn up in the form of questionnaire distributed to a cross-section of respondents. In preparing this survey questions, researchers have used a closed question. Survey questions using Likert scale format based on five categories. All categories are displayed in numerical form.

This fun question and answer the respondent to the survey easily and clearly as follows:

*Figure 2: Likert Scale*

Strongly disagree Neutral Strongly agree

1------------------------2-----------------------3-----------------------4----------------------5

Note: 1 – Strongly disagree
2 – Disagree
3 – Neutral
4 – Agree
5 – Strongly agree

The scale provided are statements about people, things or concepts and respondents should indicate how their feelings, positive or negative about the given statement (Whitely, 2002).

### 3.7 Types of Analysis

The researcher has worked with a sample to generalization and prediction, the pattern of sample from the population, the sample must represent the characteristics of population. In order to ensure that it represents the researcher used a random selection procedure, the randomly sample selected who are responding by using google form of questionnaire. There are some guiding principles adhered to conventional social science researchers. For instance, the smaller the population under study, the larger the sampling ratio. If the study population is 1000 or under, the sample ratio would need to be 30% or 300 individuals. As the population for study increases, the sampling ratio decreases. For a population of 10,000 the sample size would be 1000 (about 10%); and for populations over 150,000, smaller sampling ratios (1%) are acceptable (Neuman & Roskos, 1997). High degree of accuracy depends on the sampling ratio. For populations smaller than one thousand, a sampling ratio of 30 percent is required.

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.

### 3.7.1 Validity Test

Collins and Miller (1994) stated that the test effect on of each item is vital to the test seal constructs and items used in the questionnaire include content constructs and items appropriate of study. In this regard, any test validity that done for review based on the present-day instruments and construct is appropriate to measure variables used. If the instrument can measure with right then the instrument has the degree of the validity of the high based on content, validity of prediction and concurrent validity.

In the study, researchers have identified the existence of measurement errors on some items in constructs and questions in the interview. Improvements have been made so that Alpha's Cronbach value for each construct more than 0.65. Generally, general thinks every election tactile item in the questionnaire is match in generalize an emerging threat to banking sectors in Malaysia.

### 3.7.2. Reliability Test

The pilot studies carried out among bank’s employees at Affin Bank, Kemaman, Kuantan and Mentakab branches to assess the consistency and the degree of reliability of each item and construct in the questionnaire which was built. A total of 20 respondents are selected at random to get involved directly. The data obtained will be analyzed using the measurement's Alpha (α), using Statistical Software Package for Social

Sciences (SPSS).Alpha's Cronbach (α) can show the internal consistency of the test items in this survey with the range of 0 to 1 (SPSS Inc., 2004).

## 3.8 Pilot Test

The pilot study was to familiarize researchers with the review process prior to the actual study is carried out. The pilot study conducted by Singh and Singh (2012), intended to obtain feedback on the review instruments used as well as making improvements before the actual review is carried out. For qualitative research instruments, improvement can be done after gaining experience and feedback pilot study. While for quantitative studies on the other hand, in addition to feedback in the form of ideas, modifications can also be done with observation statistical.

Since this involves statistical analysis, arises the question of the number of required to pilot test quantitative study. Too many samples to study is not good, affect and interfere with the findings especially the storekeeper phoned researchers focus on data analysis to determine the reliability of the item. The number of samples shall be taken in accordance with the requirements of the pilot research that is not too little and not too much as well. As discussed earlier, between the purpose of the study is the analysis for estimating reliability (*reliability* research instruments, whether) the questionnaire or test items. Most popular method was by way of determining internal consistency (*internal consistency*). The SPSS package, internal consistency coefficient through predictable Cronbach *Alpha's*.

If the researcher using the number of data that many, the value of Cronbach Alpha’s automatically can be increased, which means the increase was not due to the items the questionnaire or test is good until the respondent consistent in response, but the level of consistency is obtained as the data. Researchers suggest the amount between 30 to 50 respondents is a reasonable number, ideal and accepted (acceptable). This proposal is in line with Connelly (2008), which suggests the number of samples for the study is 10 percent of the actual respondents.

In addition, Isaac & Michael (1995) and Hill (1998) have suggested sample size for study is between 10 to 30 respondents. In this regard, based on the views and many more other opinions, researchers believe that total between 30 to 50 respondents were the most reasonable. The number of respondents in this study adequate because according to Cooper and Schindler (2011), the number of respondents who fit the study is 25 to 100 respondents. While Johanson and Brooks (2010) suggests the minimum number is a total of 30 respondents to study which goal is to study early or development scale.

Researchers need to complete an inventory of questions based on previous research studies before committing to the supervisor to see consistency between the statements of the problems and objectives of the study Suter (2012) says that review this verification by supervisors is also a form of reliability data. Suter (2012) also mention that one of the validities of qualitative data is confirmation of supervisors and references selected experts on the regularity of studies conducted. After the inventory of the questions certified by the supervisor and certified by individuals who specialize in the relevant field. Researcher conducted the pilot at Affin Bank (M) Berhad Kemaman, Kuantan and Mentakab branches from 16 April 2021 to 07 May 2021. A total 40 respondents are selected and distributed the questionnaires but only 20 respondents (50 per cent) were responding the questionnaire. The respondents are selected at random in three (3) territories labelled as "Pilot Study" sent random by google form of questionnaire.

*Table 4: Total Pilot Test of Respondents of the Study*

| *Area* | *Total Questionnaire Distributed ( respondents)* | *Total Questionnaire Received (respondents)* |
|---|---|---|
| AFFIN BANK BERHAD | | |
| a) Kemaman Branch | 20 | 10 |
| b) Kuantan Branch | 10 | 5 |
| c) Mentakab Branch | 10 | 5 |
| **TOTAL** | **40** | **20 (50%)** |

The total 20 respondents provides feedback and seen by researchers several inventory questions unclear and difficult answer as needed by researchers. Therefore, the supervisor review has recommended to be researchers coordinating items and studied by researchers in accordance with the objectives of the review built. According to Khalid, Abdullah and Kumar (2012), that research should have conducted in each study quantitative patterned. Rationale for the study conducted is to ensure that the questions posed to respondents is good and can measure what is measured.

While for qualitative research conducted because there were no study questions will be improved during the interviews conducted and can be interviews again if there is information that is less clear. Questions posed next revised. A review can also be done by someone that specializes in quality management before field activities is performed. The survey was given out from 16 April 2021 until 07 May 2021 which took place three weeks' time.

## 3.9 Data Collections

*Table 4* below show the total respondents of the study. In this study, the total respondents were 123 respondents from 140 respondents (88%). The google form of questionnaire survey is distributed from 16 April 2021 until 07 May 2021, there are 123 respondents are responding.

*Table 5: Total Respondents of the Study*

| Areas | Total Questionnaire Distributed | Total Questionnaire Received |
|---|---|---|
| Affin Bank Berhad | 20 | 123 |
| Agro Bank Berhad | 10 | |
| Alliance Bank Berhad | 10 | |
| Ambank (M) Berhad | 10 | |
| Bank Islam Malaysia Berhad | 10 | |
| Bank Kerjasama Rakyat M Berhad | 5 | |

| | | |
|---|---|---|
| Bank Simpanan Nasional | 10 | |
| Bank Muamalat Malaysia Berhad | 10 | |
| CIMB Bank Berhad | 10 | |
| Hong Leong Bank Berhad | 10 | |
| HSBC Bank Berhad | 5 | |
| Maybank Berhad | 10 | |
| RHB Bank Berhad | 10 | |
| UOB Bank Berhad | 5 | |
| Public Bank Berhad | 5 | |
| **Total** | 140 | 123 (88%) |

## 3.10 Data Analysis

Data obtained are analyzed based on in statistic in a descriptive only applicable to the distribution of the frequency and the distribution of scores. For researchers an also, analyzing data inferential involves the use of various statistical methods such as the equation regress simple and double (Bougie R., 2010). This allows the decision made an overview of the in general the study population.

## 3.11 Multiple Regression Analysis

### 3.11.1 Pearson Correlation Analysis

The Pearson product-moment correlation coefficient (Pearson’s correlation, for short) is a measure of the strength and direction of association that exists between two variables measured on at least an interval scale. For example, a researcher could use a Pearson’s correlation to understand whether there is an association between exam performance and time spent revising. A researcher could also use a Pearson's correlation to understand whether there is an association between depression and length of unemployment. A Pearson’s correlation attempts to draw a line of best fit through the data of two variables, and the Pearson correlation coefficient, *r*, indicates how far away all these data points are from this line of best fit (i.e., how well the data points fit this model/line of best fit).

3.11.2. Multiple Regression Analysis is to identify changes in two or more factors contributing to the change in an independent variable. Some examples of the test conditions need to be observed as follows:

i. **Linearity**- In order to meet this requirement, all independent variables should that of the correlation in liner with variables. It can be checked via graph scatterplot in the analysis of multiple regression test.

ii. **Multicollinearity** –Such as statistical tests involving more than one other independent variables, multicollinearity exists when the There is a very strong correlation (r >. 90) between variable-Change s. in the study. One way to overcome this problem is it increases the size of the samples. It can also be identified through the value Collinearity Statistics Tolerance in the Table Excluded Variable in SPSS output. Variables are not tally with the value Collinearity less than 0.1 problematic multicollinearity.

iii. **Heteroscedasticity**- A statistic, a collection of random variables is heteroscedastic if there are sub-populations that have different variabilities from others. Here "variability" could be quantified by the variance or any other measure of statistical dispersion. Thus, heteroscedasticity is the absence of homoscedasticity.

iv. **Autocorrelation test**- Autocorrelation, also known as serial correlation, is the correlation of a signal with a delayed copy of itself as a function of delay. Informally, it is the similarity between observations as a function of the time lag between them.

### 3.12 Summary

This is the research methodology has been employed and comprehensively discussed. The discussion encompasses, research design, sampling design, survey, pilot test, process of data collection, research data instruments, type of analysis and summary of the chapter. The data analysis and result findings will be presented in next chapter.

# CHAPTER 4
# DATA ANALYSIS AND RESEARCH FINDING

## 4.0 Introduction

The background of the analysis, goals and questions of the study will be set out in the overview of this article. The scope, justification and significance of this research are also introduced in this chapter. Under this chapter, the research objectives have been spelled out as 'What are the cause of cybercrime, the risk of cybercrime and the strategy to be implemented to combat the cyber threat'. Under the literature review, the internal and external environment that affect the cyber threat. The banking environment in Malaysia and other related aspects of threat are also discussed in this paper, to highlight the real risk exposed to the users of information technology's merchandise.

## 4.1 Data Analysis

### 4.1.1 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 5* illustrate the results of each questionnaire questions, which distributed according to the study variables.

*Table 6: 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 6* 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).

### 4.1.2 Descriptive Analysis

*Table 7: 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 4.1.2 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.

### 4.1.3 Normality Analysis

Based on the result of the Normality test, all the variables are dispersion normal within in the U-shape area. This analysis was shown with the application of statistics of SPSS for the MAC version 24, found the histogram of the image and dispersion in *Figure 3*.

*Figure 3: The Histogram for Normality Analysis*
*(Dependent variable: Combating the Threat of Cybercrime)*

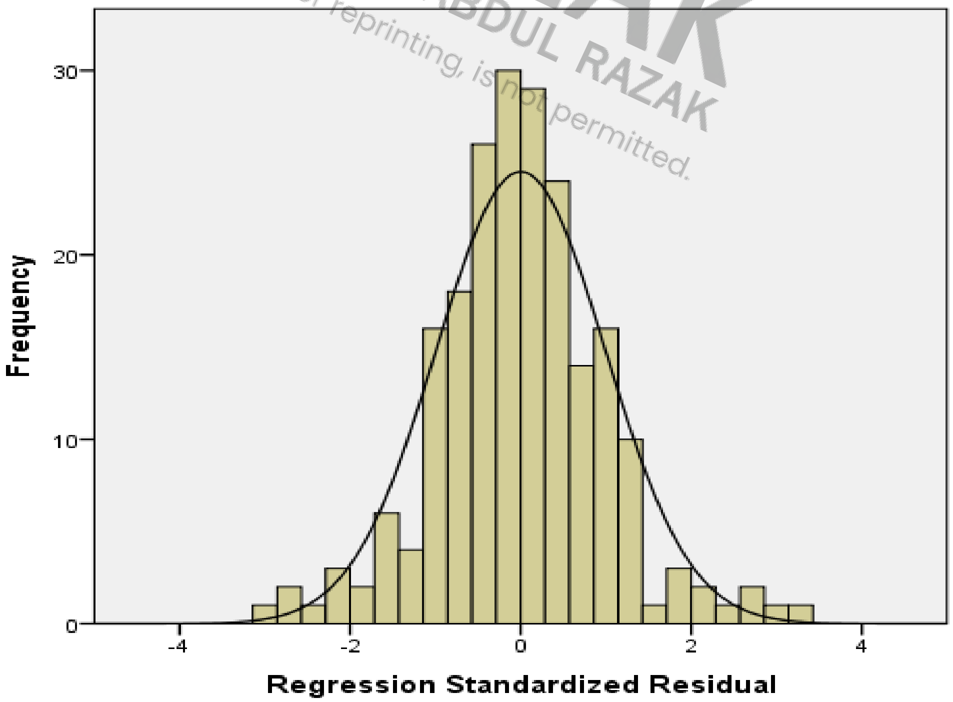


*Figure 4: Normal P-P Plot of Regression Standardized Residual (Dependent Variable: Combating the threat of Cybercrime)*

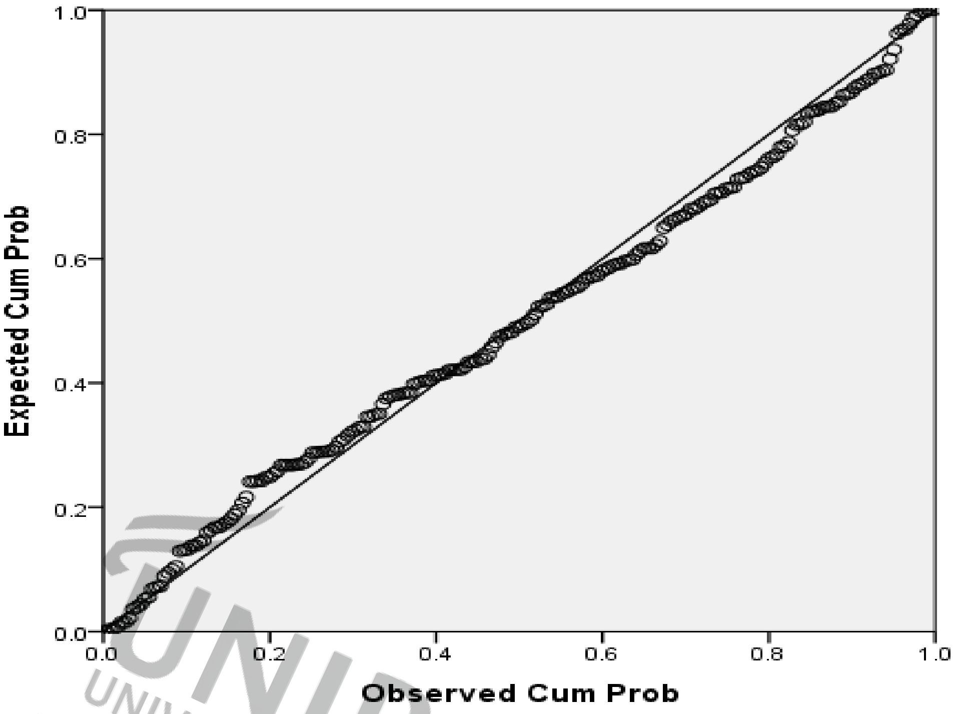
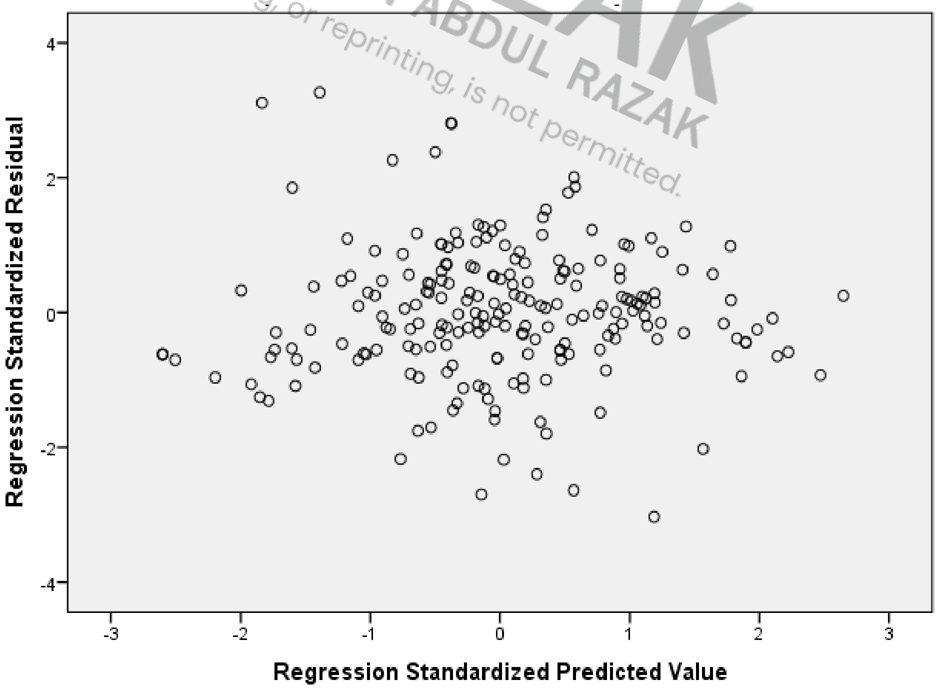


*Figure 5: The Scatter-plot for the Test of Normality*



From above *Figure 6,* the distribution of data points for each independent variable (financial literacy, public awareness, ICT & Technical tools, education and law enforcement) are scattered within the way that you and disperse around with line 45 degrees. Therefore, it follows that the multiple regression model was acceptable to fulfill the prerequisites for the normal distribution.

### 4.1.4 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 8: 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 8* 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.

### 4.1.5 Heteroscedasticity Test

Based on the results of the heteroscedasticity test with MAC SPSS applications, version 24, and Figure 6 screenshot shown below:

*Figure 6: The Scatterplot for the Heteroscedasticity Test*

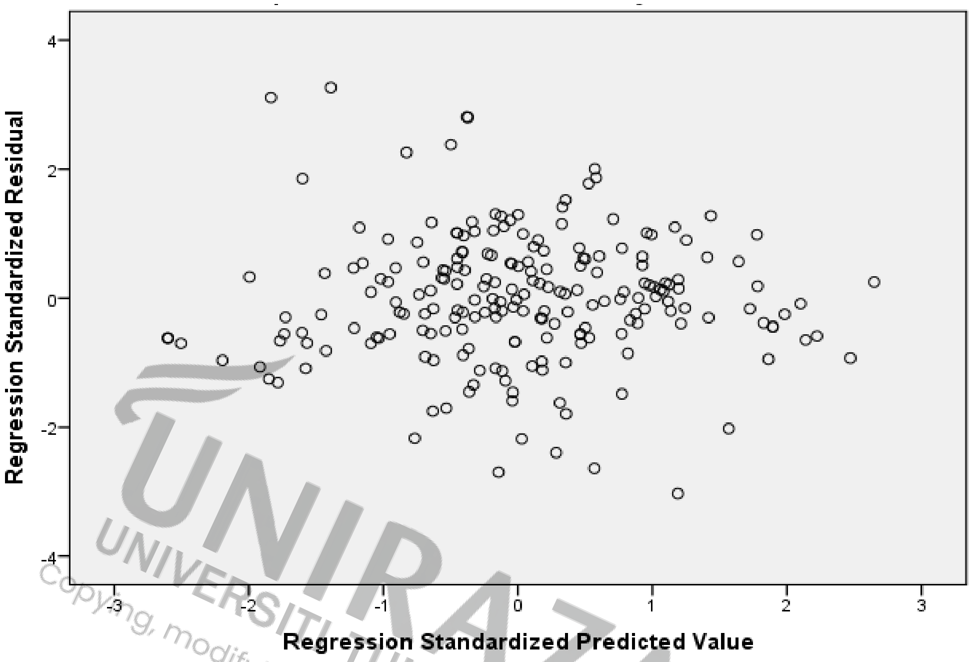


*Figure 6* shows that the data points are scattered and do not form a specific pattern for dependent variable, combating the Threat of Cybercrime in Banking Sector. Then, developed regression models there is no problem of Heteroscedasticity. Based on the analyzed data has no problem of Heteroscedasticity. The multiple linear regression equation is used for subsequent analysis.

## 4.2 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 9: 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:*

| | |
|---|---|
| *DV* | *- 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 9,* 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.

## 4.3 Multiple Regression

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 9*as per the Appendix C, spelled that 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).

## 4.4 Model Summary

*Table 10: 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 10,* Model Summary portrayed the value of R, R², and adjusted R square (R²) as well as standard error of the estimate. This model summary was done by using Enter Method. Based on the table above, the R² 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 11: 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 11* 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).

## 4.5 Hypothesis Analysis

Under hypothesis analysis, the researcher shall under all the Research Objective which has been mentioned under Chapter 1 as per the following;

i. **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.

ii. **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.

iii. **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.

iv. **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.

v. **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.

## 4.6 Summary

Based on the calculated variables, the researcher can obtain a thorough analysis of the data collected and the analysis from the IBM SPSS. The researcher would like to study the factors the mitigating factors of combating the cybercrime in banking sectors in Malaysia. The researcher understands the relationship of all the IVs towards DV. The researcher also made known which IVs that have significant influence towards the DV. To answer the first research objective, the researcher had conducted the regression analysis to see the coefficient correlation analysis in determining the relationship between the independent variables towards dependent variable.

From here, the researcher managed to identify that all the relationship are in good and strong position as the correlations are above 0.300, thus the relationships are positively good and strong. To add, all of the IVs are significant (*p*-value) at <0.001. This has indicated that the first Research Objectives and Research Questions are answered. Therefore, with all the above results, the researcher may conclude that the results derived from the study were addressed by both Research Objectives and Research Questions in this analysis.

# CHAPTER 5
# CONCLUSION AND RECOMMENDATIONS

## 5.0 Introduction

After the data were collected and analyzed, the researcher is able to examine the reliability of the objectives and the important of the variables and most prominent variables in the sample. Thus, in this chapter, the researcher will evaluate further the results and findings in Chapter Four. From there, the researcher will arrive to conclude the results and provide insights into the recommendations based on the findings of the IBM SPSS's results analysis. Besides, the research implications help to illustrate the contribution of seeking solutions to the defined problem and the relevance of the study to other parties. Limitations of the analysis have also been identified and discussed. Finally, the feasible recommendations were provided and conclude the study with recommendations for future research.

## 5.1 Conclusion

### 5.1.1. Hypotheses Testing Summary

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

*Table 12: 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 |

*Table 13* shows 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.

## 5.2 Discussion

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.

Besides external threats, the research also revealed key gaps in organizations' cybersecurity approach to protect their digital estate:

i. **Security an Afterthought**

Despite encountering a cyberattack, only 23% of organizations consider cybersecurity before the start of a digital transformation project as compared to 32% of organizations that have not encountered any cyberattack. The rest of the organizations either think about cybersecurity only after they start on the project or do not consider it at all. This limits their ability to conceptualize and deliver a "secure-by-design" project, potentially leading to insecure products going out into the market;

ii. **Creating a Complex Environment:**

Negating the popular belief that deploying a large portfolio of cybersecurity solutions will render stronger protection, the survey revealed that 15% of respondents with more than 50 cybersecurity solutions could recover from cyberattacks within an hour. In contrast, 71% of respondents with more than 11 to 25 cybersecurity solutions responded that they can recover from cyberattacks within an hour; and

**iii. Lacking cybersecurity strategy:**

While more and more organizations are considering digital transformation to gain competitive advantage, the study has shown that a majority of respondents (42%) see cybersecurity strategy only as a means to safeguard the organization against cyberattacks rather than a strategic business enabler. A mere 20% of organizations see cybersecurity strategy as a digital transformation enabler.

“The ever-changing threat environment is challenging, but there are ways to be more effective using the right blend of modern technology, strategy, and expertise,” added Mansor. “Microsoft is empowering businesses in Malaysia to take advantage of digital transformation by enabling them to embrace the technology that’s available to them, securely through its secure platform of products and services, combined with unique intelligence and broad industry partnerships.”

## 5.3 Recommendations to the Research

There are some recommendations to the research such as;

i. **Safeguard against attacks with secured software -** When you look at the on-going state of security on the internet, you must consider enhancement or complete replacement of your current protection applications. Here are some things to look at in the world of banking software development.

ii. **Security audit -** A thorough audit is imperative before any new cyber security software is implemented. The review reveals the strengths and weaknesses of the existing setup. Furthermore, it provides recommendations that can help save money while also allowing for the proper investments.

iii. **Firewalls -** Cyber security banking configuration does not only include applications. It also requires the right hardware to block attacks. With an updated firewall, banks can block malicious activity before they reach other parts of the network.

iv. **Anti-virus and anti-malware applications -** While a firewall upgrade increases protection, it won’t stop attacks unless anti-virus and anti-malware applications are updated. Older software might not contain the latest rules and virus signatures. In turn, it can miss a potentially disastrous attack on your system.

v. **Multi-factor authentication -** This protection, also known as MFA, is extremely critical to protect customers who utilize mobile or online apps to do their banking. Many users never change their passwords. Or, if they do, they make small changes. Applying MFA stops attackers from reaching the network because it asks for another level of protection. For instance, a six-digit code sent to a customer’s cell phone.

vi. **Biometrics -** This is another version of MFA even more secure than a texted code. This form of authentication relies on retina scans, thumbprints, or facial recognition to confirm a user’s identity. Though hackers have accessed this type of authentication in the past, it is more difficult to accomplish.

vii. **Automatic logout -** Many websites and apps allow a user to stay logged in if they allow it. Thus, they can access their information at any time without entering their login credentials. However, this also permits attackers to easily obtain your records. Automatic logout minimizes this by closing a user’s access after a few minutes of inactivity.

viii. **Education -**All of the above measures can increase cyber security in the banking sector. Nevertheless, they can’t help if customers continue to access their information from unprotected locations or improperly protect their login credentials. This is why education is important. When banks notify their customers of consequences related to these vulnerabilities it may move them to change their habits for fear of losing their investments.

### 5.3.1 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.

Do not click or download any links in spam emails or other messages from unidentified sources.

iii. Check the authenticity of the organizations involved by calling the companies using the number on their official website.

iv. Use strong passwords that people will not guess and do not record them anywhere.

v. 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.

## 5.4 Recommendations to the future researchers

There are some recommendations to the future researchers such as;

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 and publics. With this, the researcher will get more than 1000 respondents will participating in this study by the real and accurate result in doing the research deep from the actual sources. 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 researchers should take the consideration on the related government policies and enforcement in cybercrime. The information from BNM, Commercial banks and MCMC is valuable to analyze the issues of cybercrime in Malaysia. 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

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*. Simon and Schuster.

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment*. Sage publications.

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.

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

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*.

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

Gnaneswaran, D. (2018, July 12). Cybersecurity threats to cost organizations in Malaysia US$12.2 billion in economic losses. *Microsoft Malaysia*.

Gottfredson, M. R., &Hirschi, T. (1990). *A general theory of crime*. 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: Computer Crimes, Laws, and Policing in the 21st Century*. ABC-CLIO.

Hill, R. (1998). *The mathematical theory of plasticity* (Vol. 11). 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*. Edit publishers.

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*.

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

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*.

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

Nachmias, D. (1972). Political alienation and political behavior.

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.

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

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

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

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

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

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:*

Whiteley, A. (2002). Rigour in qualitative.

Xu, J., & Gordon, J. I. (2003). Honor thy symbionts. *Proceedings of the National Academy of Sciences*, *100*(18), 10452-10459.

# APPENDICES

# APPENDIX A

## BIOGRAPHICAL SKETCH

Wan Nora Wan Ibrahim was born on 6th of January 1966 in Dungun, Terengganu. The eldest child of a happily marriage couple of Haji Wan Ibrahim Muda and Hajjah Hasmah Abdullah. A wife to Engku Ahmad Shaifuddin Tengku Amri, the ex-Navy Officer and a mother of two lovely children who are pursuing an Aircraft Engineering License at AATC Subang and Master Programme at UiTM Shah Alam respectively. Currently, residing at own residence in Kemaman, Terengganu for the past 16 years after being transferred from Kuala Terengganu. As a village grown women who had completed the secondary level at Sekolah Menengah Sultan Omar Dungun and graduated from Universiti Teknologi Mara Dungun, living in hassle-free, clean air, peaceful and beautiful environment. The harmonized community in small town, inspire me and family to live happily and any opinion of moving to big city is neglected.

I am currently employed as a Branch Manager of Affin Bank Berhad, Kemaman, Terengganu. My first branch in Affin Bank was Kuala Terengganu, then transferred to Kemaman, Kemaman Supply Base and Kuantan. I was transferred back to Kemaman on October 2019. Prior to joining the bank, I attached to Tioxide (Malaysia) Sdn Bhd, a British Company based in Kemaman. Started to work in the bank as Customer Service Officer, incharged of opening of account, attending to enquiries, handling of ATM machines, reconciliation and administration work. After 7 years performing front office functions, I was shifted to Operations Department to manage counter works, clearing of cheques, accounts and back office work. 2 years later, I was instructed to shift to Credit Department as Credit Officer to manage credit administration works such as renewal of fire insurance, quit rent, security document, passing and balancing of accounting entries etc. My last position at Kuala Terengganu Branch was Credit Sales and Marketing Officer before transferred to Kemaman with the same position.

Due to centralization exercise of Credit Department to Kuantan, I asked to be back to Operations Department before appointed to Manager, Branch Service. After 4 years, I was appointed as a Branch Manager of which the managing of branch is under my responsibility. Of course, managing people and the branch is not an easy work. The main task which is highly expected by the management is sales of the branch, to ensure the branch is profitable and maintain viable in the market. Beside sales, the smooth running of operations, customer service and compliance have to be parallel to avoid audit issues which expose to any misconduct, losses and subsequently penalty by Bank Negara Malaysia.

Pursuing my study in Master of Business Administration (Majoring in Finance) at Universiti Tun Abdul Razak (UNIRAZAK) is an ambition for my academic enhancement and life satisfaction. At least at the end of my career, I will retire as Master of Business Administration's holder. It is also an encouragement to my children, nieces and nephews that education is forever and no one will stop us from learning. According to Lakomski, G (2001) under title organizational change, leadership and learning: culture as cognitive process from International Journal of Educational Management, spelled learning culture is cognitive process and makes brain works as sharp thinker. The neuronal pattern recognition engine allows brain to recognize all aspects of human cognition, the inner, non-symbolic as well as the outer.

APPENDIX B – QUESTIONNAIRE

## INFORMATION SHEET FOR QUESTIONNAIRE

Graduate
School of Business
UNIRAZAK

## AN EMPIRICAL STUDY ON CYBERCRIME:
## THE EMERGING THREAT TO BANKING SECTORSIN MALAYSIA

Dear Prospective Respondents,

First and foremost I would like to thank you for your attention on this survey.

I am the Master of Business Administration’s student majoring in Finance at Universiti Tun Abdul Razak, Kuala Lumpur and currently conducting a research study entitled "Cybercrime: An Emerging Threat to Banking Sectors in Malaysia". The main objective of this survey is to elucidate the most theoretically and statistically accurate factor structure of the previous developed conceptual model and to examine how individuals perceive the role of employability skills during undergraduate programs in the labor force of Malaysia. Your feedback and comments are highly valuable and needed for this study.

It takes only 5-10 minutes of your time to complete the survey. There is no right or wrong answers, only your personal opinion. For your information, the respondents' identities and feedback with regards to this survey are strictly confidential and will be used for research purposes only. When the researcher is done with the study, the researcher will write a dissertation. Your identities will not be used in the dissertation.

Your response is important to the success of the study.

Thank you and regards.

*The Researcher;*

Wan Nora Wan Ibrahim
M19711014
Master of Business Administration (Majoring in Finance)
Graduate School of Business
Universiti Tun Abdul Razak
Kuala Lumpur

*The Supervisor;*

Assoc Prof Dr Mohd Yaziz Mohd Isa
Bank Rakyat School of Business & Entrepreneurship
Universiti Tun Abdul Razak
Kuala Lumpur

## SECTION A

Graduate
School of Business
UNIRAZAK

### AN EMPIRICAL STUDY ON CYBERCRIME:
### THE EMERGING THREAT TO BANKING SECTORS IN MALAYSIA

### Background of the Respondent

*Please tick (√) on the appropriate answer;*

| ***No*** | ***Description*** | ***Answer*** |
|---|---|---|
| *1* | *Indicate your gender* | *A. Male*<br>*B. Female* |
| *2* | *Indicate your age* | *A. Below 30*<br>*B. 31 – 40*<br>*C. 41 – 50*<br>*D. 51 – 60*<br>*E. Above 60* |
| *3* | *Indicate your highest academic / professional qualification* | *A. Higher secondary*<br>*B. Graduate*<br>*C. Post graduate* |
| *4* | *How many years have you worked in the bank?* | *A. Below 5 years*<br>*B. 5 – 10 years*<br>*C. 11 – 20 years*<br>*D. Above 20 years* |
| *5* | *What is your average monthly income?* | *A. Below RM5,000*<br>*B. RM5,000 – RM10,000*<br>*C. RM10,000 – RM15,000*<br>*D. Above RM15,000* |

| | | |
|---|---|---|
| *6* | *What is your level of rank in the bank?* | *A. Clerical*<br>*B. Officer*<br>*C. Executive*<br>*D. Management* |
| *7* | *How often are you heard, experienced or being a victim of cybercrime?* | *A. Do Not Know*<br>*B. Never*<br>*C. Occasionally*<br>*D. Often* |

The End of Section A

## SECTION B

Graduate
School of Business
UNIRAZAK

### AN EMPIRICAL STUDY ON CYBERCRIME:
### THE EMERGING THREAT TO BANKING SECTORS IN MALAYSIA

### Strategies Used to Combat Financial Cybercrime

*Kindly tick (√) to indicate your level of agreement with the following attributes at the firm. Use the scale as below:*

| ***Strongly Disagree*** | ***Disagree*** | ***Neutral*** | ***Agree*** | ***Strongly Agree*** |
|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** |

| ***No.*** | ***Statement Research Variable*** | ***Strongly Disagree*** | ***Disagree*** | ***Neutral*** | ***Agree*** | ***Strongly Agree*** |
|---|---|---|---|---|---|---|
| | **FINANCIAL LITERACY** | **1** | **2** | **3** | **4** | **5** |
| 8 | *Knowledge in handling financial transactions is important in preventing cybercrime.* | | | | | |
| 9 | *Bankers carry higher weightage in combating cybercrime.* | | | | | |
| 10 | *Account holder's carry higher weightage in combating cybercrime.* | | | | | |

*Source adapted from Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017)*

| ***No.*** | ***Statement Research Variables*** | ***Strongly Disagree*** | ***Disagree*** | ***Neutral*** | ***Agree*** | ***Strongly Agree*** |
|---|---|---|---|---|---|---|
| | **PUBLIC AWARENESS** | **1** | **2** | **3** | **4** | **5** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 11 | *Public awareness helps to mitigate cybercrime.* | | | | | |
| 12 | *A culture of safety consciousness through community awareness programs should be established from young to adults.* | | | | | |
| 13 | *The effort of establishing awareness talks to banks' customers help in mitigating the cybercrime.* | | | | | |
| 14 | *Approaches used to raise cyber security awareness are still inadequate in Malaysia.* | | | | | |
| *Source adapted from Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017)* | | | | | | |
| ***No.*** | ***Statement Research Variables*** | ***Strongly Disagree*** | ***Disagree*** | ***Neutral*** | ***Agree*** | ***Strongly Agree*** |
| | **ICT TOOLS** | **1** | **2** | **3** | **4** | **5** |
| 15 | *ICT tools and prevention techniques give huge impact in preventing cybercrime.* | | | | | |
| 16 | *ICT regulators has adopted various strategies in promoting cybersecurity.* | | | | | |
| 17 | *ICT devices should be enhanced for threat detection and mitigation.* | | | | | |
| 18 | *Cybercrime Investigator / Malaysia's Computer Forensic Expert plays vital role in combating cybercrime.* | | | | | |
| *Source adapted from Farhana, S. (2020, October 25)* | | | | | | |
| ***No.*** | ***Statement Research Variables*** | ***Strongly Disagree*** | ***Disagree*** | ***Neutral*** | ***Agree*** | ***Strongly Agree*** |
| | **EDUCATION ECOSYSTEM** | **1** | **2** | **3** | **4** | **5** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 19 | *Schools and Universities are encouraged to deliver more information to educate students and raise awareness about cyber security.* | | | | | |
| 20 | *Schools and Universities are encouraged to deliver more information to educate students and raise awareness about cyber security.* | | | | | |
| 21 | *The bank needs to invest in Employee Training to train the employees to recognize a cybercrime.* | | | | | |
| 22 | *Banks' employees especially the front liners always alert on any complaints made by customers on any dispute from his/her account transactions.* | | | | | |

*Source adapted from Farhana, S. (2020, October 25)*

| ***No.*** | ***Statement Research Variables*** | ***Strongly Disagree*** | ***Disagree*** | ***Neutral*** | ***Agree*** | ***Strongly Agree*** |
|---|---|---|---|---|---|---|
| | **LAW ENFORCEMENT** | **1** | **2** | **3** | **4** | **5** |
| 23 | *The cyber security employee policy is the key resource that employee can access of they have any doubts about the cyber security.* | | | | | |
| 24 | *Law Enforcement plays a key role in implementing the cyber security priorities of our nation by examining a wide variety of* | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | *cybercrimes.* | | | | | |
| 25 | *Bank Negara and government of Malaysia are responsible in ensuring the strict law enforcement is adhered in the community of Malaysia.* | | | | | |
| 26 | *Cyber Security Malaysia has to play important role in highlighting the shortcoming of its agency due to the shortage of cyber security professionals* | | | | | |
| *Source adapted from Farhana, S. (2020, October 25)* | | | | | | |
| ***No.*** | ***Statement Research Variables*** | ***Strongly Disagree*** | ***Disagree*** | ***Neutral*** | ***Agree*** | ***Strongly Agree*** |
| | **COMBATING THE THREAT OF CYBERCRIME** | **1** | **2** | **3** | **4** | **5** |
| 27 | *Cyber threat can be mitigated through self-awareness, ICT tools, education/Training & Law Enforcement respectively* | | | | | |
| 28 | *Implementing data and password protection help to prevent cyber threat* | | | | | |
| 29 | *Combating cyber threat is the responsibility of everyone* | | | | | |
| 30 | *Banking sectors will be more reliable and trustable if the risk of cyber threat is mitigated.* | | | | | |
| *Source adapted from Hill, J. B., & Marion, N. E. (2016)* | | | | | | |

The End

## APPENDIX C – IBS SPSS TABLE

*Table 9: Multiple Regression Confident Interval*

| | | | | | | *95.0% Confidence Interval for B* | |
|---|---|---|---|---|---|---|---|
| *Model* | *Unstandardized Coefficients* | *Coefficient Std. Error* | *Standardized Coefficient Beta* | *t.* | *Sig.* | *Lower Bound* | *Upper Bound* |
| (Constant) | 3.008 | .308 | | 9.778 | <.001 | 2.399 | 3.617 |
| Financial Literacy | .147 | .089 | .233 | 1.643 | .103 | -.030 | .324 |
| Public Awareness | -.128 | .116 | -.185 | -1.103 | .272 | -.357 | .102 |
| ICT Tools | .080 | .104 | .111 | .773 | .441 | -.126 | .286 |
| Education Ecosystem | -.019 | .092 | -.023 | -.206 | .837 | -.201 | .163 |
| Law Enforcement | .293 | .103 | .388 | 2.844 | .005 | .089 | .497 |

# APPROVAL PAGE

**TITLE OF PROJECT PAPER:** **AN EMPIRICAL STUDY ON CYBERCRIME: AN EMERGING THREAT TO BANKING SECTORS IN MALAYSIA**

**NAME OF AUTHOR:** **WAN NORA BINTI WAN IBRAHIM**

---

The undersigned certify that the above candidate has fulfilled the condition of the project paper prepared in partial fulfillment for the degree of Master of Business Administration.

**SUPERVISOR**

Signature : ______________________
Name :
Date :

**ENDORSED BY:**

______________________
Dean
Graduate School of Business
Date: