

ANALYSIS OF HUMAN AND ARTIFICIAL INTELLIGENCE
INFLUENCING CYBER THREATS IN MALAYSIAN
FINANCIAL SECTORS

LAU PEI YING

ROSITA ANNE A/P RAJANTHIRAM

SABRINA BINTI ABDUL KARIM

TEOH YUAN CHI

BACHELOR OF FINANCE (HONS)

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF BUSINESS AND FINANCE

DEPARTMENT OF FINANCE

SEPTEMBER 2023

ANALYSIS OF HUMAN AND ARTIFICIAL INTELLIGENCE
INFLUENCING CYBER THREATS IN MALAYSIAN
FINANCIAL SECTORS

BY

LAU PEI YING

ROSITA ANNE A/P RAJANTHIRAM

SABRINA BINTI ABDUL KARIM

TEOH YUAN CHI

A final year project submitted in partial fulfillment of the
requirement for the degree of

BACHELOR OF FINANCE (HONS)

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF BUSINESS AND FINANCE

DEPARTMENT OF FINANCE

SEPTEMBER 2023




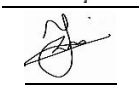
Copyright @ 2023

ALL RIGHTS RESERVED. No part of this paper may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, graphic, electronic, mechanical, photocopying, recording, scanning, or otherwise, without the prior consent of the authors.

DECLARATION

We hereby declare that:

- (1) This undergraduate FYP is the end result of our own work and that due acknowledgement has been given in the references to ALL sources of information be they printed, electronic, or personal.
- (2) No portion of this FYP has been submitted in support of any application for any other degree or qualification of this or any other university, or other institutes of learning.
- (3) Equal contribution has been made by each group member in completing the FYP.
- (4) The word count of this research report is 17430.

Name of Student:	Student ID:	Signature:
1. <u>Lau Pei Ying</u>	<u>19ABB01675</u>	
2. <u>Rosita Anne A/P Rajanthiram</u>	<u>19ABB04406</u>	
3. <u>Sabrina Binti Abdul Karim</u>	<u>21ABB00117</u>	
4. <u>Teoh Yuan Chi</u>	<u>21ABB00226</u>	

Date: 6/9/2023

ACKNOWLEDGEMENTS

We would like to express our profound gratitude to the coordinator, Puan Noorfaiz binti Purhanudin and to the supervisor, Puan Noor Azizah binti Shaari, of Universiti Tunku Abdul Rahman (UTAR), Department of Finance, for their contributions to the completion of our project titled ‘Analysis of Human and Artificial Intelligence Influencing Cyber Threats in Malaysian Financial Sectors’.

We would also like to take this opportunity to express our special thanks to our supervisor, Puan Noor Azizah binti Shaari, for her time and efforts and guidance she provided throughout the year. Your useful advice and suggestions were really helpful to us during the project’s completion. In this aspect, we are eternally grateful to you.

We are grateful to all of those with whom we have had the pleasure to work with during this and other related projects. We would like to acknowledge that this project was completed entirely by us and not by someone else.

TABLE OF CONTENTS

	Page
Copyright Page.....	ii
Declaration.....	iii
Acknowledgements.....	iv
Table of Contents.....	v
List of Tables.....	vii
List of Figures.....	viii
List of Abbreviations.....	ix
List of Appendices.....	x
Preface.....	xi
Abstract.....	xii
 CHAPTER 1 RESEARCH OVERVIEW	
1.1 Research Background.....	1
1.2 Research Problem.....	3
1.3 Research Objective and Research Questions.....	5
1.4 Research Significance.....	7
 CHAPTER 2 LITERATURE REVIEW	
2.1 Underlying Theories.....	10
2.2 Review of Variables	15

2.3 Conceptual Framework.....	25
2.4 Hypotheses Development.....	28
CHAPTER 3 METHODOLOGY	
3.1 Research Design.....	35
3.2 Sampling Design	36
3.3 Data Collection Methods.....	37
3.4 Proposed Data Analysis Tool.....	41
CHAPTER 4 DATA ANALYSIS	
4.1 Descriptive Analysis.....	43
4.2 Inferential Analysis.....	45
CHAPTER 5 DISCUSSION, CONCLUSION AND IMPLICATIONS	
5.1 Discussions of Major Findings.....	62
5.2 Implications of the Study	65
5.3 Limitations of the Study.....	71
5.4 Recommendations for Future Research.....	74
References.....	77
Appendices.....	83

LIST OF TABLES

	Page
Table 3.1: Outcome of Pilot Test	40
Table 4.1: Respondent's Demographics	43
Table 4.2: Reliability Statistics and Validity	46
Table 4.3: HTMT Output	49
Table 4.4: Collinearity Results	51
Table 4.5: Hypotheses Testing	52
Table 4.6: Determination of Coefficient (R^2)	55
Table 4.7: Determination of effect size (f)	56
Table 4.8: Determination of predictive relevance (Q^2)	57
Table 4.9: Mediation	58

LIST OF FIGURES

	Page
Figure 2.1: The fraud triangle	11
Figure 2.2: The fraud diamond model	12
Figure 2.3: Self-Determination Theory	13
Figure 2.4: Conceptual Framework	25
Figure 2.5: Research Model	29
Figure 3.1: Research flow	36
Figure 4.1: Measurement Model	45
Figure 4.2: Structural Model	50

LIST OF ABBREVIATIONS

SDT	Self Determination Theory
FDT	Fraud Diamond Theory
FTT	Fraud Triangle Theory
P	Pressure
O	Opportunity
C	Capability
R	Rationalization
AU	Autonomy
CO	Competence
RE	Relatedness
FC	Fraudulent Cases
CT	Cyber Threats
AVE	Average Variance Extracted
CR	Composite Reliability

LIST OF APPENDICES

	Page
Appendix 3.1: Questionnaire.....	83
Appendix 4.1: Original Measurement Model.....	93
Appendix 4.2: Original Reliability Statistics and Validity.....	94
Appendix 4.3: Original Specific Indirect Effects and Total Indirect Effects.....	95
Appendix 4.4: Reliability Statistics and Validity.....	96
Appendix 4.5: HTMT Output.....	97
Appendix 4.6: Collinearity.....	98
Appendix 4.7: Path Coefficients.....	99
Appendix 4.8: R Square.....	100
Appendix 4.9: f square.....	101
Appendix 4.10: Specific Indirect Effects and Total Indirect Effects.....	102
Appendix 4.11: Total Effects.....	103

PREFACE

As a part of the degree requirement and to gain knowledge in the field of finance, we are required to make a report and the topic chosen by us is ‘Analysis of Human and Artificial Intelligence Influencing Cyber Threats in Malaysian Financial Sectors’. The objective behind doing this project report is to understand in depth the influences behind cyber threats in financial sectors in Malaysia through the human and artificial intelligence factors.

This report summarizes the findings of our study on how to identify cyber threats influences in Malaysian financial sectors. We conducted survey through distributions of questionnaires and collected feedback from the surveys in order to identify the reason behind the influence.

In this report, we have included various concepts, effects, and implications regarding humans and artificial intelligence factors influence towards cyber threats in the Malaysian financial sectors. Our recommendations are based on our findings. We would like to thank everyone who contributed to this project, including our survey respondents.

Doing this project report, helped us to enhance our knowledge and broaden our perspective regarding the issues of cyber threats in the financial sectors. Through this report, we come to know about importance of understanding what causes cyber threats to occur in the financial sectors.

ABSTRACT

The use of technology has brought about a variety of changes to the financial sectors. The development of more advanced technologies has, on the one hand, made it easier for the financial sectors to carry out their regular business; on the other end of the spectrum, this has also led to an increase in the number of cyber threats. With the advent of artificial intelligence, new models for finding and avoiding cyber threat have emerged. To avoid falling prey to deception, everyone needs to educate themselves on the capabilities of artificial intelligence. Therefore, both the human and artificial intelligence perspectives have been taken into account in this research. The purpose of this study is to expand on the fraud diamond theory by providing a more comprehensive analysis of the motivations that drive dishonest individuals to engage in fraudulent behavior. On the other hand, this study also seeks to expand on the self-determination theory by bolstering pre-existing view of how characteristics that help people learn artificial technology and help the latter avoid becoming victims. In this research, we examine how human and artificial intelligence factors are related to the likelihood of cyber threats, and we speculate that fraudulent cases may play a mediator role. A questionnaire was used to obtain the data from a total of 384 adults in Malaysia. Partial Least Square-Structural Equation Modelling (PLS-SEM) software was used to analyze the collected data. We find that fraudulent cases are associated with pressure and opportunity. The findings of our paper implies that fraudulent cases influence the relationship between the two fraud risks and cyber threats.

CHAPTER 1: RESEARCH OVERVIEW

1.1 Research Background

As an essential part of Malaysia's economy and national security, the financial sector is a top target of attackers looking to take advantage of weaknesses in order to make money. Policymakers and financial institutions may put strong cybersecurity practices and technologies into place by identifying vulnerabilities and potential avenues of entry for attackers. This could be accomplished by actions like boosting network security, putting in place strict access limits, educating staff about cybersecurity best practices, and installing cutting-edge threat detection and prevention systems. (Khairuddin et al., 2020). Cyber threats continue to pose a serious threat to the sector regarding significant investments in cybersecurity technologies and practices. In order to effectively counter these attacks, it emphasizes the need for ongoing investments in cybersecurity technologies and procedures. (Mukherjee et al., 2020). By identifying these factors, policymakers and financial institutions can take proactive measures to better protect themselves against cyber threats and minimize the risk of financial losses.

Cyber threat is a deliberate attempt to access systems and networks with the intent to cause harm to people or organizations, steal sensitive information, and disrupt business processes. They can be committed by a variety of people or organizations, such as hackers, cybercriminals, actors with state support or hacktivists. Over the course of the last few decades, the financial sector has seen a dramatic rise in the frequency and severity of cyber threats in Malaysia. Cyber threat can have a variety of goals, from monetary gain and espionage to political or ideological concerns. There are numerous types of cyber threat that include malware attacks, phishing attacks and distributed denial of service attacks. There are many different types of cyber threat that fraudsters may be carried out for a number of reasons such as monetary benefits, spying, or simply

tow a line in the status quo. Cyber threat can have major repercussions, from the loss of private or financial information to the interruption of vital infrastructure or public services. Strong security measures must be put in place by individuals and companies, including encryption, strong password, regular software upgrades, and employee education and training in order to reduce the danger of cyber threat. In the interest of responding swiftly and effectively to any potential cyber threat, it is also crucial to have a detailed incident response plan in place.

In the field of cyber threat, computers are the tools utilized by both attackers and defenders. Computers are the means by which both attackers and defenders are able to launch attacks and thwart them, but it is people working behind the scenes of machines that actually engage in fraud. Without a human being involved, computers cannot start fraud on their own. Fraud often involves people who use technology for personal benefit, take advantage of weaknesses, or deceive others. Computers and other digital equipment may be used by them to carry out their criminal actions, such as financial fraud, identity theft, or data breaches. These people frequently have specialized knowledge, skills, and evil intent to take advantage of vulnerabilities in systems or mislead victims who are unaware. On the other hand, in order to identify, stop, and deal with fraud, defenders like cybersecurity experts and fraud detectives also rely on computers and technology. These people use innovative instruments, data analytics, and security measures to spot and stop fraudulent activity.

During the past few years in Malaysia, there have been a number of instances of notable fraud cases that have been documented. Since the first reported attack in 1990, phishing attacks have evolved into a highly sophisticated attack vector and are now considered one of the most common forms of internet fraud. Victims of these attacks may suffer significant losses, including the theft of sensitive information, identity theft, and the loss of company and government secrets (Alkhalil et al., 2021). According to the experts, networked artificial intelligence will increase human effectiveness while also

endangering human autonomy, agency, and capabilities. They discussed the numerous possibilities, including the possibility that computers might match or even surpass human intelligence and capabilities on tasks like complex decision-making, reasoning, and learning, as well as sophisticated analytics and pattern recognition, visual acuity, speech recognition, and language translation (Atske, 2022). The vast majority of them are con artists who take part in fraudulent activities, although some of them are most likely to be taken advantage of themselves by unscrupulous others. The growing number of instances of fraud in Malaysia is having a substantial impact on the country's alarming growth in the frequency and severity of cyber threats.

1.2 Research Problem

Cyber threat is referred to as any hostile act or activity that aims to interfere, harm or obtain unauthorized access to a device, system or network. Cyber threats pose an enormous risk to individuals, firms, governments and also the economy of the country (Wadha Abdullah Al-Khater, 2020). Isaac Wiafe stated that any criminal activity that uses technology or other forms of communication to inflict fear and anxiety, harm or damage is referred to as cyberthreats (Isaac Wiafe, 2020). Malaysia's financial sector faces numerous cyber threats, just like those faced by other countries. Cyber threats have significantly increased in the financial sector over the past few decades. According to the crime statistics Malaysia, 2022 it is being reported the number of commercial crime cases in 2021 has increased to 15.3%, indicating that it is still on the rise. In contrast to the 283 cases recorded in 2020, there were 400 cases of cybercrime reported to the Royal Malaysian Police in 2021 (Malaysia, 2022). The Bank Negara Malaysia Annual Report 2020 states that cyber threats have continued to rise in frequency and complexity in the financial sector of Malaysia, with financial institutions serving as their main target. A total of 3,759 cyber threats were recorded in 2020, a 47% increase from the previous year (Bank Negara Malaysia, 2021).

The aim of this research is to examine how fraud cases in Malaysia's financial sectors have a bearing on the influence of human and artificial intelligence on the cyber threat. Thus, the interfering mechanism of this research study is the fraudulent cases. In Malaysia, there have been a number of high-profile fraud cases recorded in past years. According to the Criminal Code and other pertinent regulations, fraud is a crime in Malaysia that carries a prison sentence and a financial penalty. Financial fraud in the financial sectors is one of the frauds that are frequently reported in Malaysia. It could be seen from the crime statistics in Malaysia that it has recorded the highest number of cases in 2021 at 28,842 fraud cases (Malaysia, 2022). The majority of them are fraudsters who engage in fraud whereas some are most likely to become the victims of fraud. The rise in cyber threats in Malaysia is significantly impacted by the number of fraudulent cases. Fraudulent cases could mediate the relationship between human factors (pressure, opportunity, rationalization and capabilities) and cyber threats, by providing insight into the mechanism or process by which certain factors lead to an increased probability of cyber threats. Contrasted with, fraudulent cases could mediate the relationship between artificial intelligence factors (autonomy, competence and relatedness) and cyber threats, by shedding light on the system or procedure through which a particular factor reduces the likelihood of cyber threats. Given the psychological factors that encourage fraudsters to commit crime, Malaysia has seen a rise in the total number of crime cases annually (Vousinas, 2018). Whereas with the aid of artificial intelligence technology, the incidence of cases ought to decline (Qi Xia, 2022). Which brings us to the research study's objective, which is to comprehend how human and artificial intelligence factors affect the cyber threats in the financial sectors of Malaysia.

In this research we decided to conduct a study in order to further investigate the relationship between human and artificial intelligence and the risk of cyber threats, which has resulted in fraudulent cases in Malaysia's financial sectors. Both the human and artificial intelligence variables have a positive and negative impact on the cyber threats in Malaysia's financial sector. The study's research gap is the utilization of

fraudulent cases as the study's interfering mechanism. This is due to the fact that previous studies or research that has been done has not been addressed fraudulent cases as their interfering mechanism. It is crucial to investigate the impact of human and artificial intelligence on the cyber threat as it relates to fraud cases in Malaysia's financial sectors. Apart from that, we applied self-determination theory in this study to further investigate how artificial intelligence factors influences cyber threats. Previous financial sector studies have not looked into this theory in depth. This theory sought to understand more on how artificial intelligence learning is impacted by cyber threats. This brings back to the study's main objective, which is to investigate how cyber threats in Malaysia's financial sector are influenced by both human and artificial intelligence factors.

1.3 Research Objectives & Research Questions

1.3.1 Research Objectives

The objective of this research is to examine how both the human and artificial intelligence factors influence cyber threats in Malaysian financial sectors. In consideration of the research purpose, the following objectives are crucial and ought to be covered in this study:

1. To investigate the relationship between human factors (i.e., pressure, opportunities, rationalisation, capabilities) and cyber threats in the financial sectors of Malaysia.
2. To investigate the relationship between artificial intelligence factors (i.e., autonomy, competence, relatedness) and cyber threats in the financial sectors of Malaysia.

3. To investigate the mediating effect of fraudulent cases in the relationship between human factors (i.e., pressure, opportunities, rationalisation, capabilities) and cyber threats in the financial sectors of Malaysia.
4. To investigate the mediating effect of fraudulent cases in the relationship between artificial intelligence factors (i.e., autonomy, competence, relatedness) and cyber threats in the financial sectors of Malaysia.

1.3.2 Research Questions

Based on the research objective mentioned above, the aforementioned research questions could provide information on the research objectives. The research question of this study is to examine how both the human and artificial intelligence factors influence cyber threats in Malaysian financial sectors. The following questions are pertinent to this study and should be addressed in light of the aforementioned problems:

1. Is there any significant relationship between human factors (i.e., pressure, opportunity, rationalisation, capabilities) and cyber threats in the financial sectors of Malaysia?
2. Is there any significant relationship between artificial intelligence factors (i.e., autonomy, competence, relatedness) and cyber threats in the financial sectors of Malaysia?
3. To what extent do fraudulent cases mediate the significant relationship between human factors (i.e., pressure, opportunity, rationalisation, capabilities) and cyber threats in the financial sectors of Malaysia?
4. To what extent do fraudulent cases mediate the significant relationship between artificial intelligence factors (i.e., autonomy, competence, relatedness) and cyber threats in the financial sectors of Malaysia?

1.4 Research Significance

A significant aspect of Malaysia's economy and national security, the financial industry is a prime target for criminals wanting to exploit loopholes and make a profit. Due to the fact that it deals with actual problems and offers useful suggestions and ideas, the research study on cybersecurity in Malaysia's financial sector is significant from a practical standpoint. This study provides insights that can aid in solving issues in the real world by examining the human factors that motivate fraudsters to engage in fraud as well as the function of artificial intelligence in avoiding fraudulent conduct. This study contributes to the resolution of several problems that exist in the real world, including the human aspects that can potentially drive fraudsters into committing fraud. In order to create successful prevention and detection techniques, it is essential to understand the motivations of fraudsters. This study can help policymakers, financial institutions, and law enforcement authorities develop targeted interventions and preventive measures by illuminating the human factors that may motivate fraudsters to participate in fraudulent activities. With the use of this information, it will be easier to spot weaknesses, deal with the underlying issues, and put protective measures in place to stop and catch fraudulent activity. On the other hand, the artificial intelligence aspects provide victims with useful ideas and suggestions to help them avoid being involved in fraudulent activity. Financial institutions can improve their ability to spot and stop fraudulent activity by utilizing AI technologies. This is done by analyzing massive volumes of data and looking for patterns and anomalies that can point to fraudulent behaviour. Moreover, the results of the research can also be used to inform people and increase awareness of potential fraud threats, arming them with information and advice to prevent becoming victims. This study will demonstrate that human and artificial intelligence factors have both a positive and a negative impact on the financial sectors in Malaysia. It emphasizes the necessity of a complete strategy that integrates the capabilities of AI technologies with human judgment, skill, and ethical issues. The results of this study will presumably educate the people of Malaysia regarding the

numerous instances of financial fraud that have recently been brought to light. It offers useful suggestions and insights that may be used by different stakeholders to address pressing issues, inform the public about financial fraud, and create strong defenses for the financial system and its stakeholders.

This study provides valuable insights for future researchers interested in the field of cybersecurity in Malaysia. The analysis of human and artificial intelligence factors that affect cyber threats in the financial sector of Malaysia will help to further our understanding of cybersecurity in the country. By looking more closely at the elements that were found and how they affect cyberthreats in the financial sector, future researchers can improve on the findings of this study. They can investigate extra facets of human behaviour, such as engineering strategies or psychological elements that support fraud. Researchers can also learn more about the function of artificial intelligence and how well it works to identify and stop cyberthreats in the financial sector. This study provides an analysis of the human and artificial intelligence factors that will influence cyber threats in the financial sector of Malaysia. Moreover, this study also offers useful information for future researchers interested in this related topic. This study may help in enhancing the researcher's understanding of the factors that influence cyber threats in the financial sector of Malaysia. This study will investigate how fraudulent cases act as the interfering mechanism between these factors and cyber threats in Malaysia's financial sector. The results of this study will provide insights into the variables that influence cyber threats and the countermeasures that can be applied.

Furthermore, by investigating how fraudulent cases act as the interfering mechanism between these factors and cyber threats in Malaysia's financial sector, this study can provide a better understanding of the dynamics at play in cybersecurity incidents. This knowledge can then be used to develop countermeasures that are more effective in preventing cyber threats in the financial sector. The danger of cyber risks can be

reduced, for example, if financial institutions improve their fraud detection and prevention systems to spot suspected fraudulent activity early on. This study can provide policymakers, financial institutions, and other stakeholders with information on how to better protect against cyber threats by identifying the factors that influence cyber threats in Malaysia's financial sector (Nor et al., 2020). Lastly, the impact of this study can be seen in its potential to make Malaysia's financial system safer and more secure. By providing insights into the factors that influence cyber threats and the countermeasures that can be applied, this study can help to mitigate the risks posed by cyber threats, benefiting both the country's economy and its citizens.

CHAPTER 2: LITERATURE REVIEW

2.1 Underlying Theories

The use of information technology enhances and improves the financial sectors in many ways. The technology offers advantages, but it also has its drawbacks. In Malaysia, the digital market is expanding daily and cyber threats are forging ahead. Cyber threat is an issue that emerges as a result of the quick adoption of information technology. Given the vast amounts of data and money they store, financial institutions are a prime target for cyber-attacks. Cyber threats can either directly or indirectly have an impact on the entire society. It is challenging to tell who really is striking us and whether the attackers are machines or people. Therefore, precautions should be taken because these are the new aspects of network attacks.

2.1.1 Fraud Diamond Theory

Cyber threats can be understood better by first recognizing the motivations behind these threats. The first theory that is involved in this study is the “Fraud Diamond Theory”. The fraud triangle (Figure 2.1) is the most commonly used theory to explain why people commit fraud. This is a model that was created in 1953 by criminologist Donald Cressey, whose research focused on embezzlers, or what he termed as “trust violators”.

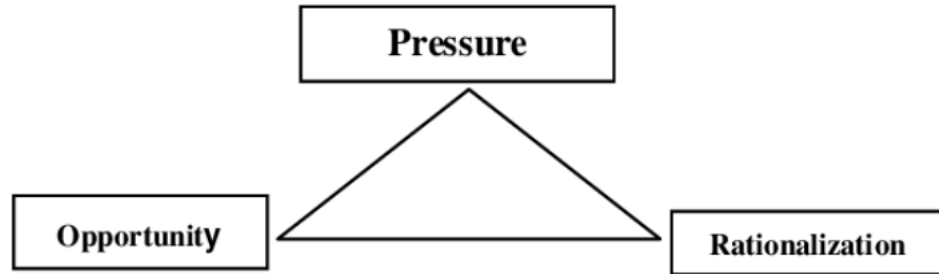
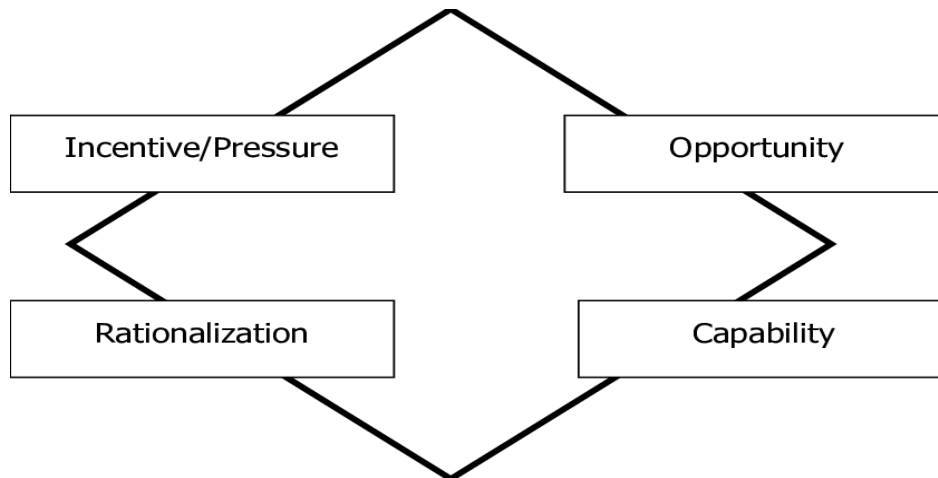


Figure 2.1. The fraud triangle. Adapted from Wells, J. T. (2005). *Principles of fraud examination*. Hoboken, New York: John Wiley and Sons

According to this theory, fraud is inconceivable without these three components, and the degree of each component determines how significant the fraud is (Dorminey, 2012). A perceived non-shareable financial need is represented by one of the triangle's legs. The second leg stands for perceived opportunity, while the last leg represents rationalization. Most studies indicate that fraud is more likely to occur when someone has an incentive (pressure) to commit fraud, when supervision or weak controls give them an opportunity to do so, and when they can justify their fraudulent action (Wolfe & Hermanson, 2004). Cressey's theory explains that people who are trusted turn into trust violators when they think they have this issue. The second point of the fraud triangle is perceived opportunity. The theory states that, by itself, a non-shareable financial issue won't motivate an employee to commit fraud. A breach of trust must involve all three elements. The ability to conduct fraud is what is meant by the perceived opportunity leg. Opportunity explains a person's willingness to take part in a scam. Rationalization is the third and last element of the fraud triangle. The act of rationalization is a prerequisite to the commission of the crime. Rationalization is the process by which someone explains away their dishonest behaviour. The embezzler must defend his wrongdoing before he ever acts on it, because he does not see himself as a criminal. (Vousinas, 2019)



*Figure 2.2. The fraud diamond model. Adapted from Wolfe, D. T. and Hermanson, D. R. (2004). *The Fraud Diamond: Considering the Four Elements of Fraud*.*

According to Wolfe and Hermanson (2004), adding a fourth element to the fraud triangle could increase fraud detection. The fraud diamond theory (Figure 2.2) was first introduced by Wolfe and Hermanson in December 2004. The authors' four-sided fraud diamond addresses pressure, opportunity, rationalization, as well as an individual's capability, which is a crucial factor in determining whether fraud will actually happen even when the other three aspects are present. A lot of frauds, particularly some of the multi-billion dollar ones, would not have happened in the absence of the proper person with the right capabilities in place. Capability explains the abilities or information required to execute the scam. According to them, an offence can only happen if all four elements - pressure, opportunity, rationalisation, and capability - are satisfied. Individuals and organizations can work to spot and stop fraudulent behaviour before it happens by understanding the fraud diamond theory and how it applies to the financial sector. As well as encouraging an ethical and open culture, this may require stricter financial controls and supervision measures. (CFI Team, 2023)

2.1.2 Self-Determination Theory

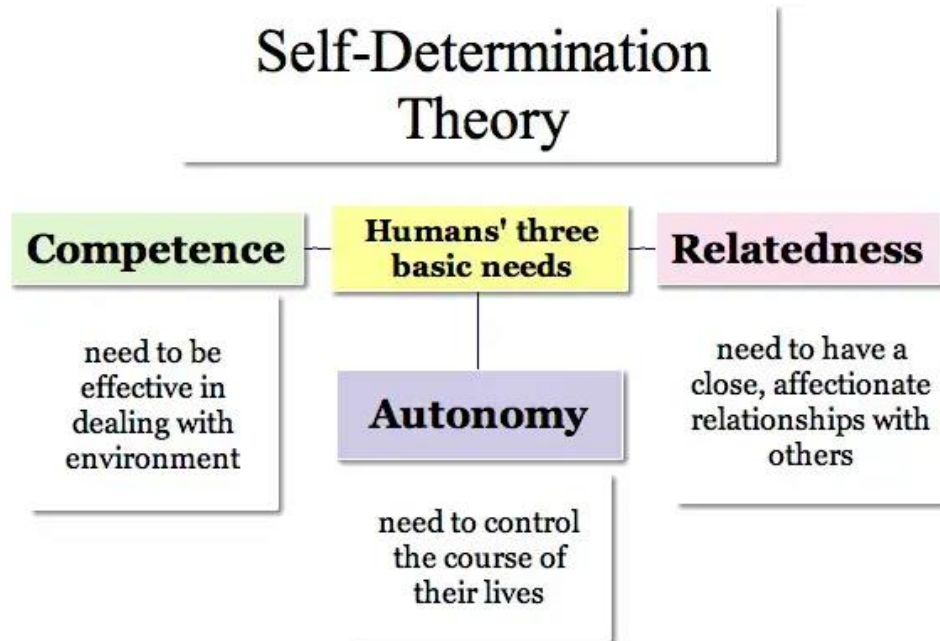


Figure 2.3. Self-Determination Theory. Adapted from Courtney E. Ackerman, (2018). *Self Determination Theory and How It Explains Motivation*.

Self-determination theory (SDT) is a motivational theory that explains the factors that influence an individual's motivation and behavior. According to Self-determination theory, individuals have three basic psychological needs such as autonomy, competence, and relatedness. When these needs are satisfied, individuals are more likely to be intrinsically motivated and involved in their activities (Cherry, K. ,2022). Self-determination theory could be used to understand the motivational variables that influence individuals to engage in cyber threats in the context of the analysis of human and artificial intelligence (AI) factors that influence cyber threats in Malaysia's financial sector. For instance, an employee in the financial sector may be more likely to participate in cyber threats as a means of getting control or demonstrating their abilities if they feel that their autonomy or competence is being disputed. Furthermore, Self-determination theory can also be used to investigate how AI is involved in cyber threats. For example, if the design of an AI system prevents employees from exercising

their autonomy or competence, this might potentially result in employee disengagement and even resistance, which could then raise the possibility of cyber threats.

According to self-determination theory, further explanation of three essential components that individuals must feel in order to achieve psychological growth and well-being: autonomy, competence, and relatedness. The feeling of being in control of one's own actions and decisions is referred to as autonomy. Individuals who have a sense of autonomy feel empowered and are more likely to take the initiative and participate in activities that are consistent with their personal values and goals. Autonomy can be fostered by providing individuals with options and opportunities to make their own decisions. Secondly, the sense of accomplishment and mastery that result from learning and developing new skills is referred to as competence. Individuals who feel competent are more likely to take on new challenges and persevere in the face of adversity. Competence can be developed by providing opportunities for individuals to learn and grow, as well as feedback that reinforces their progress and success. Third, relatedness or connection, refers to a sense of belonging and connection to others. Individuals who feel connected to others feel a sense of support and validation, which helps them navigate life's challenges. Creating opportunities for social interaction and promoting a sense of community and shared values can help to foster relatedness. Autonomy, competence, and relatedness work together to create a powerful framework for promoting psychological growth and well-being. People are more likely to thrive and feel that their lives have meaning and purpose when they feel in control of their lives, competent in their abilities, and connected to others (Cherry, 2022).

2.2 Review of Variables

2.2.1 Dependent Variable

The dependent variable that is referred to as a variable that is measured or observed as part of this research study is the **cyber threats**. According to the author (Raheela Firdaus, 2022), the findings demonstrated that the fraud diamond theory and the properties of artificial intelligence had positive and substantial influence on cyber threats. Isaac Wiafe stated that any criminal activity that uses technology or other forms of communication to inflict fear and anxiety, harm or damage is referred to as cyberthreats (Isaac Wiafe, 2020). Malicious actions known as “cyber threats” aim to compromise computer networks, systems, and devices in order to commit fraud, obtain information, create havoc or impede operations. It may acquire in a wide variety of forms, such as viruses, malware, phishing, ransomware and others. Cyberthreats is any illicit activity carried out online or through a computer that can have the potential to harm people, organizations, governments and affect financially (Wadha Abdullah Al-Khater, 2020).

In a world where concerns of cyber threats are growing daily, the financial sector has witnessed an increase in fraud. Fraudsters are the ones that engage in fraudulent activities with the purpose of misleading, defrauding, or stealing from others. They can deceive their victims into parting with money or personal information by employing various strategies like phishing, identity theft, scams and other ruses. Fraudsters can conduct their operations offline or online, and they may have a variety of targets, including people, firms or even governments. A vital potential for fraudsters to reap the benefits of and carry out fraud is due to the systemic vulnerabilities. Katelyn explained due to the epidemic, COVID-19, numerous services were moved online,

which is why cyber frauds were expanding along with it (McKinnon, 2022). Many retail businesses were compelled to cease operations as a result of the COVID-19 epidemic lockdowns, which had a negative influence on the industry. Substantially limiting face-to-face service in businesses, retail businesses routinely conduct their operations through online services. The digital technology that underpins the online way of life has long been prevalent, but since the start of the pandemic, its growth has exploded (Cameron Guthrie, 2021).

A logical increase in the usage of digital technologies has been brought on by the COVID-19 epidemic. We could observe that following the epidemic, cyber frauds were becoming much more active than before. It has created an environment of uncertainty that is enticing fraudsters to take advantage of the crisis by obtaining and exposing information of victims (Rahul De', 2020). Rahul De' has also mentioned that many users are starting to rely primarily on technologies, whereas some are first time users who are increasingly falling prey to frauds. This has also led to an upsurge in fraud in the financial sectors. Cyber threats have incredibly advanced causing the ineffectiveness of the defences. This illustrates that human and artificial intelligence factors could have a significant impact on cyber threats.

2.2.2 Independent Variable

There are two independent variables to examine its impact on the dependent variable used for this research study which is **human factors and artificial intelligence (AI) factors**. The factors that can influence the impact of human and artificial intelligence and human physiology on cyberthreats in the financial sector are known as independent variables. Human psychology could be significant in minimizing fraudulent cases by

identifying strange behaviour activities of a human. Whereas, on the other hand artificial intelligence could be used to prevent and identify fraudulent activities. In this study of human physiology, which applies the fraud diamond theory focusing on humans' pressure, opportunities, rationalization and capabilities while artificial intelligence applies the self-determination theory focusing on the autonomy, competence and relatedness. In order to study the impact of both human physiology and artificial intelligence on cyber threats in the financial sector, equal emphasis has been given in this research study.

When it comes to committing fraud, **human physiology** is a major factor. Fraud diamond theory is used in order to identify humans' physiology which is human's pressure, opportunities, rationalization and capabilities in committing fraud (Vousinas, 2018). Computers are unable to breach a system without human interference since they are the ones who operate the computers in the back which leads to committing fraud. By influencing their emotions, beliefs, and habits, fraudsters frequently take advantage of the shortcomings and vulnerabilities of their victims (Raheela Firdaus, 2022). In order to create effective prevention and detection measures, it is essential to comprehend the physiological elements that lead to fraud. Even though discovering fraud in the financial sector might be challenging, human physiology can be helpful in identifying any unusual behaviour and averting fraudulent activities. We can lessen the risk that people may fall victim to fraud by teaching them about typical fraud schemes and the tricks employed by fraudsters. Thus, understanding human physiology is essential in stopping these atrocities.

Many factors, including greed, financial pressure, a lack of ethics, or the desire to uphold a specific way of living, can lead to fraud instances in the financial sector. According to Cressey, **pressure** is a non-shareable financial issue or an inducement for dishonesty. Pressure may be brought on by the need to achieve goals or expectations, the need to hide financial problems, or the desire to make money for oneself in the

financial sector. People may be driven to commit fraud by a variety of factors, including human pressure. As stated by (Raheela Firdaus, 2022) the pressure that employees in an organization apply to one another often results in fraudulent activity. Thus, people may feel pushed to conduct fraud as a result of their own financial issues, such as increasing bills, bad credit, or unanticipated expenses. To relieve their financial burden or to preserve their standard of living, people may turn to fraudulent activities in these circumstances. As per (Sunardi, 2018), financial fraud was more likely to occur in organizations with significant levels of financial instability and external management pressure. Peer pressure is another type of human pressure in which people may be persuaded to commit fraud by their superiors or co-workers. This can happen at work places when there is a culture of cutting corners, hitting goals no matter what, or where the organization's ethical standards are poor. People could feel pressured to commit fraud if they worry about losing their jobs or feel they must fulfil inflated performance standards imposed by their employers. Employees may feel compelled to commit fraud in order to meet their objectives as a result of this pressure (Jiang, 2022). This pressure leads them to use unethical shortcuts, which can lead to a stressful work environment. Financial sector employees may experience pressure to reach goals, timelines, or standards imposed by management or the business.

Another key component that gives fraudsters the ability to perpetrate fraud is the **opportunity**. A person's willingness to participate in a fraud can be explained by opportunity (Vousinas, 2018). In the financial sector, this could provide access to financial data or systems and have the power to alter financial transactions or records. Fraudsters may take advantage of holes in internal controls or flaws in the organization's rules and procedures. If there is an opportunity and lack of supervision at their organization, fraudsters will commit fraud. Some authors have asserted that financial fraud is impossible without an opportunity, even under extremely stressful circumstances. Ach Maulidi brought forward that, when considering fraud cases from an opportunity standpoint, it is not mandatory to demonstrate that there has to be an opportunity before a fraud can indeed be perpetrated (Maulidi, 2020). The capability

and potential of an individual to identify the flaws in the organizational structure and exploit them by committing fraud. Employees who have access to financial data, for instance, could misuse their position of power by falsifying financial reports or embezzling money. This not only, if given the chance, fraudsters will use their skills to commit fraud in the financial sectors. According to (Mansor, 2018), the possibility of fraud increases a person's willingness to engage in fraudulent behaviour when it is present in an organization. opportunities exist when surveillance or monitoring procedures are not used, or when management's efforts to prevent opportunities for potential fraudsters are shown to be lacking. Fraud seems to be more likely to take place on average, when the risk detection is minimal.

Rationalization, which is the explanation of a behaviour as a usual event that is ethically right in a typical culture. This enables a person to keep up their perception of themselves as a reliable individual (Vousinas, 2018). This could promote explaining the deception to make a means of making amends for previous wrongdoings or to ensure the company's survival in the financial sector. In essence, part of what motivated the crime was the justification. An embezzler is unable to recognize themselves as a fraudster and therefore must defend their wrongdoings prior to the moment they commit fraud. According to the author Sunardi, fraud and rationalization go hand in hand. One of the main causes of fraudsters occurring in the financial sector had been identified as inadequate compensation, which could serve as the justification for engaging in committing fraud (Sunardi Sunardi, 2018). An insightful explanation of views regarding the use of rationalization had been made by some authors. They demonstrated that the influence of the attitude on misstating is stronger when the Machiavellian level is high. The range of an individual's character traits is constrained and defined by the situation of the actions in which they had performed, regardless of whether they ought to be associated with rationalization or any negative emotion (Maulidi, 2020). Individuals who engage in fraud frequently explain away their actions by citing personal or financial pressures, perceived injustices, or the notion that they

are entitled to the assets or money that has been taken from them. If a fraudster is unable to justify their dishonest actions, they are less inclined to conduct fraud.

A person's propensity for fraud and their place within an organization is denoted by their **capabilities**. According to Georgios, capability is the term used to describe the character traits and skills that are crucial in determining if fraud will actually happen in the face of pressure, opportunity, and rationalization. If there aren't any suitable individuals with the proper skills executing the intricacies of the fraud, most of the frauds might not have taken place in the financial sector (Vousinas, 2018). A great deal of huge fraud is highly unlikely to occur if there aren't any employees in the business with unique skills. Opportunity arrives at the doorstep yet rationalization nudges the potential fraudsters in the direction of the doorway, however the person must be capable of getting through all of it (Edy Sujana, 2019). Fraudsters might possess the information, abilities, and technological resources necessary to carry out their deception but capability plays an essential role in doing so. Christine has shown a positive correlation between capabilities and frauds in the financial sectors (Agbanyo, 2020). Since changes in directors can result in an initial performance that is subpar due to the phase of adjustment, this serves as a proxy for the capacity to detect the incidence of fake financial statements (Rani Eka Diansari, 2019). In the financial sector, this could involve understanding accounting theories or financial systems, as well as the capacity to illegally manipulate financial information or transactions. A lack of moral or ethical norms that would forbid them from acting dishonestly is another factor that may apply.

Due to the obvious number and complexity of financial transactions that take place every day in the financial sector, it is particularly prone to fraud. With the analysis of massive volumes of data and the detection of trends or anomalies that may be indicative of fraudulent behaviour, **artificial intelligence (AI)** can play a crucial role in both detecting and preventing fraud. This study has looked into AI aspects, such as the

autonomy, competence and relatedness that can be used to lessen cybercrime (Qi Xia, 2022). In order to prevent being a victim of fraud, artificial intelligence learning is essential for everyone. AI has turned out to be a helpful tool for detecting and preventing fraud in the financial sectors. Massive amounts of data may be rapidly and precisely analysed by AI algorithms (Anand, 2021). This effective analysing enormous volumes of data, artificial intelligence can assist the financial sector in discovering any fraudulent activities. The wealth of many consumers is at stake in the financial industry; therefore, solutions are expensive but effective. Securing the cost of the system with AI is cost-efficient management since it requires less human engagement and training modules. As a result, engagement and well-being are boosted when the three fundamental psychological demands of autonomy, competence, and relatedness are met. Those that provide learning activities that address these three concerns will be able to encourage more victims to participate in strengthening their AI skills in order to protect themselves from cyberthreats.

Autonomy, is a person's degree of freedom in mastering AI depends on his or her own initiative. Victims should be encouraged on their independence by putting themselves in charge of their own learning and initiatives in choosing their own preference learning path, where the skills related to AI that is deem useful based on their personal discretion (Qi Xia, 2022). An individual has the right and capacity to decide and take action in accordance with his or her own principles, priorities, and goals on becoming an expert in AI. Artificial intelligence (AI) is causing a seismic shift in the financial sectors thus those that take the initiative to gain the knowledge on AI and continue to keep up with the latest developments will be in a stronger position to remain with the trends and take advantage of new opportunities as they arise. A person's sense of agency is crucial because it motivates them to act in ways that best serve themselves. Conversely, people need to believe that they can shape their own destinies and that they have some control over their own life (Ackerman, 2018). A person's susceptibility to cyber treats increases if they fail to stay up with the latest developments in AI in the financial sectors. Individuals who are self-motivated and take the initiative to seek out and gain

knowledge are able to mold their own learning experience in AI, which is an immense swiftly expanding field.

The capacity of an individual to carry out its intended activities accurately and efficiently is referred to as **competence**. Victims are less invested in, competent at, and confident in their AI abilities, and they value such abilities less for what they're worth (Qi Xia, 2022). A likely explanation for this outlook is because victims believe the educational opportunities they are receiving do not welcome and included them as fully as they would like. In addition, competence can also be influenced by number of other factors, such as the quality of the data used to train a person on AI, the difficulty of the tasks it is designed to perform, and the expertise of the system's developers and operators. To be competent in AI is to be able to perform it confidently and successfully. Every individual has to acquire the necessary skills and the ability to understand the AI is the sort of knowledge and skills that can be considered part of one's competence. Therefore, there is a need for every individual to develop their skills and take charge of their lives in ways that are meaningful to them. Victims would need to develop their skills in AI to the point where they will never get involved in fraud schemes. There are several specialised areas of expertise that must all be mastered in order to fully understand AI. When victims feel that they are capable of grasping AI applications, they are intuitively more likely to believe that they have a greater chance of being able to lead an autonomous life in the AI era, have the ability to foster positive social change with AI, and may keep discovering more about AI. This is because victims who consider that they are capable of comprehending AI applications have a greater tendency to think that they are highly competent to lead an independent lifestyle in the AI generation (Ching Sing Chai, 2020). This requirement concerns our abilities, insights, and experience (Courtney E. Ackerman, 2018).

The term "**relatedness**" is used to describe a person's level of connection to and participation in their wider social community. Victims are more likely to engage in

learning and have less of a sense of isolation if they are made to feel safe, accepted, and linked to AI, and if they build strong personal networks capable of providing help and support. The problems of diversity and inclusiveness in artificial intelligence learning may be fixed if the needs were met (Qi Xia, 2022). One's sense of relatedness may not depend solely on how they feel about their own interactions with other people; it may also depend on how they would like to relate to other people or things, such as connecting with AI. A tool that measures relatedness and includes a subscale measuring the desire to contribute was shown to be reliable and valid (Ching Sing Chai, 2020). Contributing to greater benefit of society and maintaining strong understanding on AI are essential components of social well-being. The results of these studies lend credence to the idea that victims' propensity to utilise AI could contribute to their sense well-being. This could occur, for example, if victims see that artificial intelligence technologies give them the freedom to act independently and the motivation to study more about AI. By promoting collaboration across various systems and information sharing about potential threats, relatedness may be important for preventing cyber threats. Being connected to others will help those who have suffered trauma. Victims are more invested in their education when they have a positive experience, and when they are able to build strong personal networks that can provide assistance and support, all of which are facilitated by the modern world's ubiquitous artificial intelligence. If these requirements are met, the artificial intelligence's diversity and inclusion problems may be solved. Due to this, it is necessary for people to feel that they are connected to and a part of the community around them because we are all, to some extent, reliant on the actions and interactions of other people.

2.2.3 Mediator Variable

The mediator variable of this research study is **fraudulent cases**. The mediator variable is a variable that explains the relationship between two other variables (Frendy, 2022). It is a fictional variable that is used to describe the relationship between the independent

and dependent variable. Fraudulent cases may serve as a mediator in the relationship of human and artificial intelligence factors that lead to the probability of cyber threats in Malaysia's financial sector. This implies that fraudulent cases can aid in the explanation of how factors of both human and artificial intelligence influence the occurrence of cyber threats. For example, fraudulent cases could mediate the relationship between pressure and cyber threats, by providing insight into the mechanism or process by which certain pressure leads to an increased probability of cyber threats. There have been several high-profile cases of fraud documented in recent years. The fraud that commonly makes headlines in Malaysia is financial sector fraud. According to crime data, in 2021, Malaysia had the most cases, at 28,842 fraud cases that had been filed, of any country in the world (Malaysia, 2022).

The overall number of annual crimes committed in Malaysia has been on the rise. The vast majority of them are dishonest people who commit fraud, while others are likely to be taken advantage of themselves as the victims (Vousinas, 2018). The growing number of fraudulent cases in Malaysia has had a major impact on the escalation of cyber threats in the country. If the internal control systems of a company also include weaknesses or gaps that make it simpler for individuals to engage in fraudulent cases such as embezzlement or money theft. For instance, employees could be able to take advantage of these gaps to commit fraud if an organization does not have adequate systems in place for monitoring financial transactions (Frendy,2022). Therefore, the probability of fraud cases arising could increase as a result of this situation, which would increase the risk of cyberthreats in the financial sector. On top of that, fraudsters have a much better chance of succeeding with their schemes of their targets have a poor understanding of how artificial intelligence operates. The usage and comprehension of artificial intelligence in the financial sector may not lead to disinterest or apathy on the part of workers. Due to this, there is a greater potential for fraud to occur, which in turn increases the vulnerability of the financial sector to cyber threats.

In conclusion, the mediator variable is an important concept in this research since it contributes to a more complete understanding of the mechanisms or processes that contribute to the relationship between variables. By shedding light on the mechanism or process by which certain circumstances increase the chance of cyber threats, fraudulent cases may serve as a mediator between human factors and cyber threats. On the other hand, fraudulent cases may operate as a mediator between artificial intelligence factors and cyber threats, illuminating the system or procedure by which a particular component mitigates cyber risks. The relationship between human and artificial intelligence factors and the occurrence of cyber threats in the financial sector appears to be mediated through fraudulent cases. Therefore, researchers can create more efficient prevention and intervention strategies to solve the cyber threats and lessen the probability of fraudulent cases in the financial sector by studying the function of fraudulent cases as a mediator variable.

2.3 Conceptual Framework

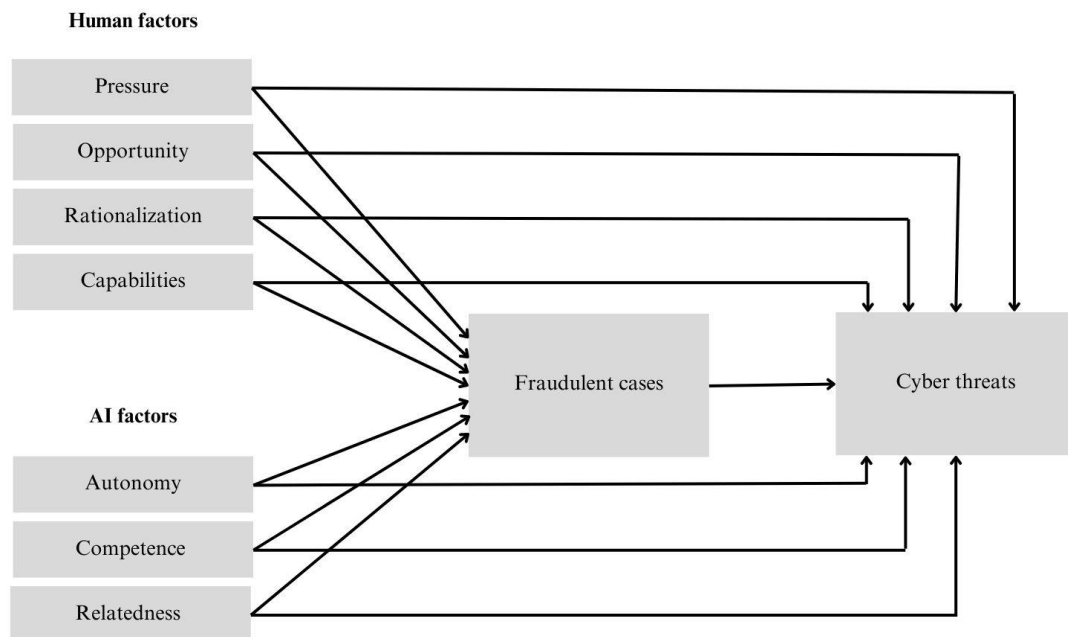


Figure 2.4. Conceptual Framework

Understanding and addressing the unique cybers threat challenges faced by Malaysian financial institutions requires the integration of human and artificial intelligence. As smart devices become more common in smart connected homes, the implications for cybersecurity and the vulnerabilities of these devices must be investigated. There is an increasing need to address the security threats posed by devices in connected smart homes, even though research has primarily concentrated on the defense mechanisms of corporate and national infrastructures. The demand for smart device interconnectivity introduces new risks that must be managed to ensure user protection. To develop strategies to improve fraudulent cases in Malaysia's financial sector by analyzing the interaction between human actions, artificial intelligence, and cyber threats (Mishra, 2023).

In this study, cyber threat serves as the dependent variable. Cyber threats are malicious activities that target computer systems, networks, or electronic devices with the intent of causing harm or stealing sensitive information. To effectively address the growing threat of cyber threat, it is critical to have a thorough understanding of the various factors that contribute to their occurrence. Cyber threats issues are influenced by the shortcomings of artificial intelligence as well as the motivation level of people to commit fraudulent activities. A conceptual framework can help to analyse and organise complex phenomena by breaking them down into component parts and identifying the relationships between them. Informing the creation of efficient strategies and policies to prevent, detect, and respond to cyberattacks requires an understanding of the complex and dynamic nature of cyber threats (Tunggal, 2022). For the purpose of preventing, detecting, and responding to fraudulent activities in the context of cyber threats, developing effective strategies requires an understanding of these two factors; human factors and artificial intelligence factors. It can develop a more comprehensive and effective approach to combating cyber threats by addressing both the human and artificial intelligence factors involved in fraudulent cases. Ineffective defenses are

direct result of the remarkable progress made by cyberthreats. This demonstrates how considerations including both human and AI could have a major bearing on the severity of cyber threats.

Human factors and artificial intelligence (AI) factors are the independent variables. Human factors are psychological and behavioral factors that can influence people to commit fraud. This may involve elements like pressure, opportunity, rationalization, and capability (Vousinas, 2018). Even though detecting fraud in the financial sector might be a tough job, human psychology can be effective in spotting suspicious behavior and preventing fraudulent cases. It could also identify people who are more likely to engage in fraudulent behavior or who are likely to fall victim to it (Raheela Firdaus, 2022). Artificial intelligence (AI) factors can reduce the victims who are exposed to fraud. This may involve elements like autonomy, competence, and relatedness (Qi Xia, 2022). AI is becoming more sophisticated and is being used more frequently in cyberattacks. For victims, AI can provide tools and resources for detecting and preventing fraud or cyber threats, giving them a greater sense of control over their financial security. Additionally, AI can enable victims to report incidents of fraud or cyber threats anonymously, without fear of retaliation. In this research study, equal emphasis has been given to both human and AI in order to explore the influence that cyber threats can have on the financial sector.

The purpose of this study is to investigate how instances of fraud in Malaysia's financial sectors might be used to draw conclusions about the roles played by human physiology and artificial intelligence in the development of cyber threat vulnerabilities. Therefore, the incidents of fraudulent activity are the mediator through which this research study is conducted. The rapid increase in the number of instances of fraud that have been reported in Malaysia has had a significant influence on the progression of the cyber threats that have been reported in the country. When there are holes or weak spots in an organization's internal control mechanisms, it becomes easier for dishonest

employees to steal money through embezzlement or other forms of fraud. In addition, if victims don't grasp how AI works, fraudsters have a considerably better chance of succeeding with their schemes. Thus, the potential for fraud cases to emerge may expand as a result of this situation, heightening the threat posed by cyberthreats to the financial sector. Fraudulent cases may mediate human factors and cyber threats by revealing how particular situations raise the likelihood of certain cyber threats. It also mediates between AI and cyber threat, revealing how a component reduces cyber risks. As conclusion, this research relies on the mediator variable to better understand the mechanisms that link variables.

2.4 Hypotheses Development

This study investigates the relationship between fraud human factors (pressure, opportunity, rationalization, and capabilities) and cyber threats and as well the relationship between artificial intelligence factors (autonomy, competence, and relatedness) and cyber threats. In addition, this study examines the mediating effect of fraudulent cases in the relationship between the four elements of fraud human factors and three elements of artificial intelligence factors with cyber threats (Figure 2.5).

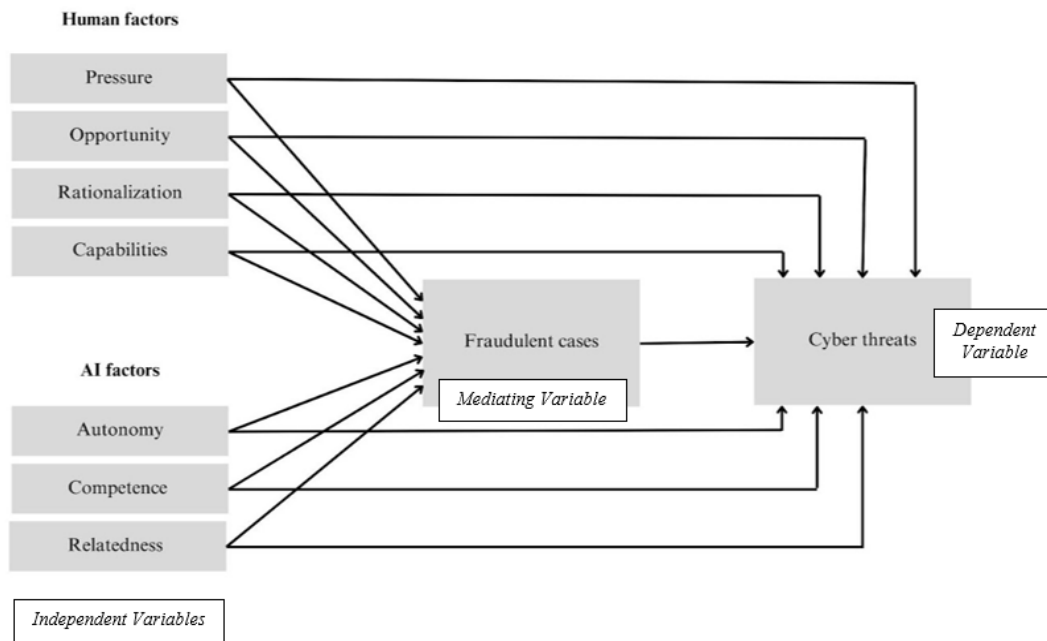


Figure 2.5. Research Model.

2.4.1 Human factors and cyber threats

2.4.1.1 The relationship between pressure and cyber threats

Perceived pressure is a crucial motivator for fraud. Pressure is defined as financial and non-financial constraints on individual members of an organization that can be derived from environmental, social, financial, and political factors (Mangala & Soni, 2022). Depending on the pressure, it could be either financial or non-financial. The most common cause of negative behavior by institutions or individuals is financial pressure. More particular, almost 95% of all fraud cases are driven by cash demands made on the fraudsters. Greed, spending above one's means, major debt, health or financial concerns in the family, and gambling are all examples of perceived pressure. The form

of financial pressure differs based on the fraud perpetrator's role and status (Kazemian, 2019). Personal pressure is the most motivating factor for low-level employees, whereas external or work-related pressures are more motivating for medium and upper-level employees (Mangala & Soni, 2022). Based on the theory above, the first hypotheses is formed:

H1a: There is a significant relationship between pressure and cyber threats.

2.4.1.2 The relationship between opportunity and cyber threats

Opportunity can explain a person's desire to assist in a deception (Vousinas, 2018). Fraudsters will commit fraud if there is an opportunity and a lack of oversight in their organization. Financial fraud, according to some authors, is impossible without an opportunity, even under severely stressed conditions. According to (Mansor, 2018), the presence of fraud in an organization boosts a person's desire to engage in fraudulent transactions and activities. Therefore, the second hypotheses is formed:

H1b: There is a significant relationship between opportunity and cyber threats.

2.4.1.3 The relationship between rationalization and cyber threats

As per the human fraud diamond theory, the third element is rationalization. According to Kazemian et al. (2019), a rationalization is an act used by fraud offenders to excuse their fraudulent conduct as normal and morally acceptable, as well as to defend themselves by claiming they have no other alternative. Employees that commit fraud with the argument that they only borrow money from the bank are examples of rationalization in banking fraud. Several other fraud committers have rationalized their

fraudulent acts as a result of their low salary (Kazemian et al., 2019). Hence, the third hypotheses is formed:

H1c: There is a significant relationship between rationalization and cyber threats.

2.4.1.4 The relationship between capabilities and cyber threats

According to Wolfe and Hermanson (2004), the human fraud diamond theory does not adequately describe the nature of fraud and so is insufficient to prevent and detect occurrences of fraud. As a result, they included a new aspect called capability, which refers to a person's position in the organization that gives them the potential to exploit a fraud opportunity. According to Kazemian et al. (2019), fraud committers are intelligent people who recognizes and exploit internal control flaws and use their position to earn benefits by committing fraud. The third element, opportunity, alone is insufficient; instead, fraud perpetrators must have sufficient competence to take advantage of the scenario. This leads to the formation of the fourth hypotheses:

H1d: There is a significant relationship between capabilities and cyber threats.

2.4.2 Artificial intelligence and cyber threats

2.4.2.1 The relationship between autonomy and cyber threats

The degree of freedom a person has in mastering artificial intelligence (AI) is determined by his or her own initiative. Artificial intelligence (AI) is causing a seismic shift in the financial sectors, so those who take the initiative to learn about artificial

intelligence (AI) and stay up to date on the latest developments will be in a better position to stay on top of trends and capitalize on new opportunities as they arise. People, on the other hand, need to think that they have some influence over their own lives and that they can mold their own destinies. Therefore, the following fifth hypotheses is formed:

H2a: There is a significant relationship between autonomy and cyber threats.

2.4.2.2 The relationship between competence and cyber threats

Competence refers to an individual's ability to carry out their intended activities accurately and efficiently. Artificial intelligence (AI) competence means being able to conduct it confidently and successfully. Every individual must learn the required skills, and understanding artificial intelligence (AI) is an example of knowledge and skills that can be regarded part of one's competency. As a result, every individual must develop their abilities and take control of their lives in a way that are significant to them. Hence, sixth hypotheses is developed:

H2b: There is a significant relationship between competence and cyber threats.

2.4.2.3 The relationship between relatedness and cyber threats

The feeling of relatedness may not be entirely determined by how they see their personal relationships with other people; it may also be determined by how they wish to relate to other people or objects, such as engaging with artificial intelligence. Victims see that artificial intelligence technologies provide them the freedom to act autonomously and the drive to learn more about AI. Relatedness may be useful for

preventing cyber risks by enabling collaboration across diverse systems and information sharing about potential attacks. Victims are more invested in their education when they have a positive experience and can create strong personal networks that can provide assistance and support, all of which is assisted by the modern world's pervasive artificial intelligence. This brings to the seventh hypotheses being formed:

H2c: There is a significant relationship between relatedness and cyber threats.

2.4.3 Mediation of fraudulent cases in the relationship between human factors and cyber threats

The mediator variable, fraudulent cases, explains the relationship between the independent variable and dependent variable. Fraudulent cases serve as the mediator in the relationship of human factors that lead to the probability of cyber threats in Malaysian financial sectors. This shows that fraudulent cases can aid in the explanation of how factors of human influence the occurrence of cyber threats. Fraudulent cases could mediate the relationship between pressure, opportunity, rationalization and capabilities with cyber threats, providing insights into the process by which these factors lead to an increased probability of cyber threats. Therefore, four hypotheses are formed here as followed:

H3: There is a significant relationship between fraudulent cases and cyber threats.

H3a: Fraudulent cases does mediate the relationship between pressure and cyber threats.

H3b: Fraudulent cases does mediate the relationship between opportunity and cyber threats.

H3c: Fraudulent cases does mediate the relationship between rationalization and cyber threats.

H3d: Fraudulent cases does mediate the relationship between capabilities and cyber threats.

2.4.4 Mediation of fraudulent cases in the relationship between artificial intelligence and cyber threats

Fraudulent cases have higher chances of occurring and fraudsters have higher chances of succeeding in their fraud plans towards the targets that have a very poor or less understanding of how artificial intelligence works in real world. Hence, there is a greater possibility of fraud occurring, increasing the financial sector's sensitivity to cyber threats. Three hypotheses can be derived to understand the relationship between fraudulent cases and self-determination factors towards cyber threats:

H4a: Fraudulent cases does mediate the relationship between autonomy and cyber threats.

H4b: Fraudulent cases does mediate the relationship between competence and cyber threats.

H4c: Fraudulent cases does mediate the relationship between relatedness and cyber threats.

CHAPTER 3: METHODOLOGY

3.1 Research Design

The method employed in this study was a quantitative research method, which involves quantifying and analyzing variables to get results. The chosen research design was descriptive research to test the four objectives. Descriptive research is known as a methodical procedure of observing and recording what a subject does without affecting them. It is a theory-based design approach that is developed through the collection, evaluation, and presentation of data. Surveys, interviews, case studies, and observations are examples of methods. Descriptive research is best used for collecting unbiased information that indicates behaviors or repeating events (Romanchuk, 2023). In this study, human and artificial intelligence serves as the independent variables and whereas cyber threats serve as the dependent variable, followed by a mediator which is fraudulent cases.

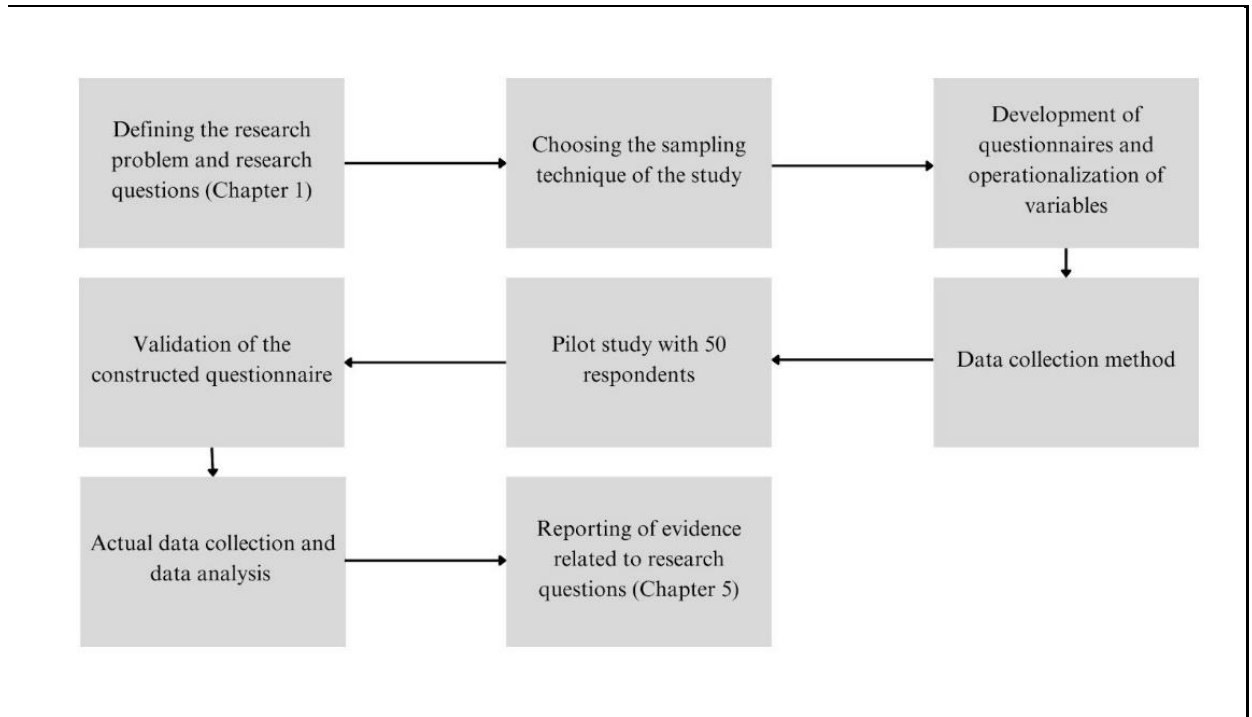


Figure 3.1. Research flow.

3.2 Sampling Design

This study is set to be carried out in Malaysia. This study's notable target population are individuals who are aged between the range of 18 to 55 years old in Malaysia. The reason behind the chosen range of age for this study is to identify the working adult's population. In Malaysia, the composition of the population aged 15 to 64 are known as the working age. According to a report released by global provider of analytics software, FICO, 62% of Malaysians are willing to commit fraud to get a loan or make an insurance claim (Birruntha, 2023). Malware and intrusion accounted for 95% of cyber occurrences in Malaysia in the first half of 2022, while fraud continued to be the most frequent and fastest-growing incidence (Mardhiah, 2023). Furthermore, based on the data by Malaysian Anti-Corruption Commission, the age range of 36 to 45 is where

the majority of offenders are found. However, the majority of losses are caused by older people. One rationale is that positions in high management have unrestricted authority and easy access to the resources of the company. The younger generation is under pressure, whereas older, more seasoned individuals have greater possibilities (Satar, 2019). Hence due to the statistics mentioned, this study emphasizes on studying the particular age range of Malaysians to further understand their contribution and effect towards fraudulent cases and cyber threats in the financial sectors of Malaysia.

The sampling technique used was convenience sampling where it is a non-probability sampling technique where units are chosen for the sample based on their accessibility to the researcher. This may be as a result of close proximity geographically, availability at a specific moment, or willingness to take part in the study. Convenience sampling, which is sometimes referred to as accidental sampling, is a kind of non-random sampling (Nikolopoulou, 2022). A sample size of 384 respondents from Malaysia is chosen. The reasoning behind this sample size is based on the Krejcie and Morgan table, where for a population size, N , of more than 1000000, a sample size, S , of 384 people will be chosen. By using the Krejcie and Morgan table to choose the sample size, the researcher does not need to conduct research on each sample. In order to create a quantitative study for research, this method would be very helpful.

3.3 Data Collection Methods

In this study, primary data is used to collect and analyze the information. Primary data includes first-hand information that has not been published (Crowther, 2012). The research instrument used in this study is in the form of a questionnaire. The questionnaire was created because it is the quickest and easiest way to get quantitative data from a large number of respondents.

3.3.1 Questionnaire Instruments

The cover page of the questionnaire includes a brief statement of this study's purpose. The questionnaire survey consists of two parts. The first part or Section A of the questionnaire is to collect background or demographic information of the respondents. The information required are gender, age, academic qualification, current work position, monthly income, and number of years of work experience. This is due to an individual's choices, interests, and actions within particular businesses, such as the financial sectors can be influenced by this demographic information's. As an example, different ages have different risk tolerance. Investing and retirement planning strategies may differ depending on the age group. Younger individuals might place a greater emphasis on growth-oriented investments, whereas older individuals would place a higher priority on security and income generation. Therefore, retirement planning, estate planning, and money preservation may be more important to older people. When it comes to financial transactions, investments, and banking, younger age groups may be more at ease with and receptive to using technology, whereas elderly people may show greater caution or have different preferences. The effect of fintech and the use of artificial intelligence in financial services are two examples of developing trends in the financial sectors that may be seen differently by different age groups.

The second part of the questionnaire which consists of the dependent variable, independent variables, and mediator, is divided into four sections; Section B, C, and D, with a total of 36 questions, to obtain information on the cyber threats, human factors, artificial intelligence factors, and fraudulent cases. As for the second part of the questionnaire, a five-point Likert scale was used to measure each variable in this study, with 1 denoting strongly disagree, 2 denoting disagree, 3 denoting neither agree or disagree, 4 denoting agree, and 5 denoting strongly agree. The list of questions used in the questionnaire is included in the Appendix.

The questionnaire instruments have been adapted from previous studies. In order to analyze the human and artificial intelligence factors impacting the cyber threat, questionnaires based on the one created by Kazemian (2019) and Salameh (2021) were constructed. The questionnaire developed by Kazemian was used to develop questionnaires to assess cyber threats, and the human factors which are pressure, opportunities, rationalization, and capabilities. Four questions for each variable of human factors and four regarding cyber threats were adapted from Kazemian. Pressure related questions were developed to gauge the degree to which both financial and non-financial pressure such as their insolvency or their working environment presents flaws that could lead to the occurrence of fraud. Questions on opportunities were implemented after being modified to reflect the potential that might occur for an individual to be inclined to commit fraud. Rationalization might be cited as an explanation for their justification of deception. Capability is where it determines an individual's abilities on both how likely they are to commit fraud and where they fit within the organization. This study used modified versions of artificial intelligence questions that were taken from Xia (2022, Rahman (2021) and Salameh (2021). Adapted from Xia and Rahman were four questions for every variable of artificial intelligence. The extent of an individual's choice in learning artificial intelligence questions is measured by autonomy. Questions on competence measure a person's capacity for encouraging themselves in learning artificial intelligence. Individual interpersonal interaction in artificial intelligence is measured by questions in relatedness. Based on Kazemian and Rahman's research, four questions were created to gauge the extent of influences on fraudulent cases from human and artificial intelligence factors.

3.3.2 Pilot Study

Pilot study is crucial as it helps in the improvement of the research's quality and effectiveness (In, 2017). In addition, it also ensures that the respondents value the

questionnaire intended to be used in our study. For the purpose of pilot study, a total of 50 samples of questionnaires (refer Appendix 3.1) were given to the respondents. In this study, it is determined that a pilot test ought to have at least 9% of the sample size of the main respondent collection by using a one-sided confidence interval with a significance level of 80% (Kim Cocks, 2013). Pilot study is crucial as it helps in the improvement of the research's quality and effectiveness (In, 2017). In addition to this, it assures that respondents value the questionnaire that is going to be used in our research, which is a huge plus. In order to carry out the pilot study, each responder was given one sample questionnaire, bringing the total number of questionnaires sent to 50.

The validity test for this study is done through the convergent validity tests. The convergent validity tests provide information on the Average Variance Extracted (AVE) values where if it is more than 0.50, then it indicates an acceptable convergent validity. A reliability analysis verifies the measurement's validity and foundation. Cronbach's alpha, the most used reliability statistic, was utilized in our study to assess the consistency of variables on a summarized scale. The internal consistency of a set of items, or how closely connected they are to one another as a group, is measured by Cronbach's alpha. It is regarded as a gauge of the reliability of the scale. When the Cronbach alpha is more than 0.7, the research's instruments are considered reliable (Taber, 2018). When the Cronbach alpha is more than 0.7, the research's instruments are considered reliable (Taber, 2018).

Table 3.1:

Outcome of Pilot Test

Construct	Cronbach's Alpha
Pressure	0.809
Opportunity	0.679

Rationalization	0.645
Capability	0.801
Autonomy	0.759
Competence	0.720
Relatedness	0.616
Fraudulent Cases	0.692
Cyber Threats	0.720

For the purpose of carrying out the pilot test, a total of 50 respondents were collected. Google form was utilised to collect the 50 respondents' responses. After that, the Cronbach's alpha test was utilised for the purpose of testing. The composite reliability values fall within the acceptable range of the standard construct reliability, which is greater than 0.70. Whereas the Cronbach alpha shows that only few of the variables are more than 0.70.

3.4 Proposed Data Analysis Tool

The data collected through the questionnaires were analyzed using the SmartPLS software. In a moderately complicated research model that includes independent, mediating, and dependent variables, Partial Least Squares-Structural Equation Modelling (PLS-SEM) technique is employed to investigate the relationship between unobserved or latent variables (Hair et al., 2017). A descriptive analysis of respondents' demographics is conducted to ascertain the number of respondents tested for gender, age, academic qualification, current work position, monthly income, and work experience. In order to examine the questions about human factors, artificial intelligence factors, fraudulent cases, and cyber threats, an inferential analysis is carried

out where means and standard deviations will be used to analyze the variables. Regression analysis is also used to test the relationship between the predictors of human and artificial intelligence and at the same time to examine the effect of mediator fraudulent cases in the relationship of human and artificial intelligence towards cyber threats. Regression analysis is evaluated to ensure the overall model is significant. The purpose of this analysis is to determine the magnitude and direction of the influence of every independent variable on the dependent variable and followed by the hypotheses testing.

CHAPTER 4: DATA ANALYSIS

4.1 Descriptive Analysis

Table 4.1

Respondent's Demographics

Variable	Category	Frequency	Percentage
Gender	Male	197	51.3%
	Female	187	48.7%
Age	18-25 years old	215	56.2%
	26-30 years old	55	14.2%
	31-40 years old	73	19.1%
	41-50 years old	23	5.9%
	55-55 years old	18	4.6%
Academic Qualification	SPM/ Certification	80	20.9%
	Diploma	75	19.6%
	Bachelor's Degree	199	51.8%

	Masters/ Doctorate	30	7.7%
Current Position/ Work Designation	Unemployed	169	44.1%
	Top management	46	12.1%
	Middle management	60	15.7%
	Supervisor	30	7.7%
	Support staff	45	11.6%
Monthly Income	Less than RM999	170	44.3%
	RM 1000 - RM 2999	97	25.3%
	RM 3000 - RM 4999	76	19.8%
	RM 5000 and above	41	10.6%
Number of Years of Work Experience	Less than 1 year	185	48.2%
	1-5 years	90	23.5%
	6-10 years	79	20.6%
	10 years and above	30	7.7%

Based on the demographic information obtained from the 384 respondents, it can be seen that there is a 51.3% population of male which is more than number of females. Furthermore, the majority of respondents age falls under the age group of 18 to 25 years old, who are considered as young adults, accounting for 56.2% from the overall. Most of the respondents' highest academic qualification is degree and out of the 384 respondents, 15.7% of them work in the middle management. 44.3% of respondents agrees that their salaries are less than RM999, which may be a factor that leads to committing fraud.

4.2 Inferential Analysis

4.2.1 Measurement Model Assessment

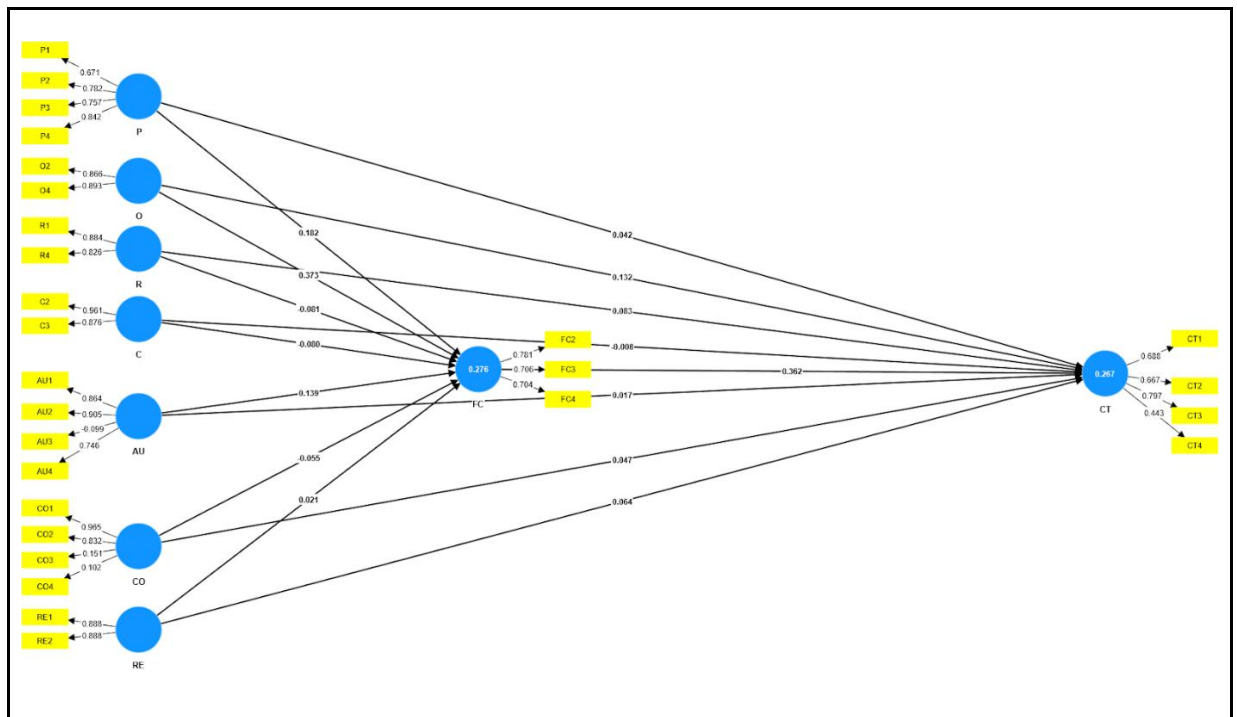


Figure 4.1. Measurement Model

4.2.1.1 Indicator Reliability

Table 4.2

Reliability Statistics and Validity

Construct	Item	Loading	CR	AVE
P	P1	0.671	0.849	0.586
	P2	0.782		
	P3	0.757		
	P4	0.842		
O	O2	0.866	0.872	0.774
	O4	0.893		
R	R1	0.884	0.845	0.732
	R4	0.826		
C	C2	0.961	0.917	0.846
	C3	0.876		
AU	AU1	0.864	0.758	0.533

	AU2	0.905		
	AU3	-0.099		
	AU4	0.746		
CO	CO1	0.965	0.642	0.414
	CO2	0.832		
	CO3	0.151		
	CO4	0.102		
RE	RE1	0.888	0.881	0.788
	RE2	0.888		
FC	FC2	0.781	0.775	0.535
	FC3	0.706		
	FC4	0.704		
CT	CT1	0.688	0.750	0.437
	CT2	0.667		

	CT3	0.797		
	CT4	0.443		

4.2.1.2 Internal Consistency Reliability

Table 4.2 shows that the composite reliability values for all the constructs except for the Competence (CO) construct, falls within the acceptable range of the standard construct reliability, which is more than 0.70. Similar to Cronbach's alpha, composite reliability also known as construct reliability is a measure of internal consistency in scale items (Netemeyer, 2003). Upon removal of certain items from certain constructs, the internal consistency reliability shows better improvement in terms of composite reliability and AVE values, as shown in Table 4.2. The original measurement model (refer Appendix 4.1) that consists of complete set of items in all constructs, shows a very low values of AVE and composite reliability of less than 0.4 for both, for the constructs of independent variables; Opportunity (O) and Rationalization (R). (refer Appendix 4.2)

4.2.1.3 Convergent Validity

Based on Table 1, the Average Variance Extracted (AVE) values for all constructs are above 0.5, except for the Competence (CO) and Cyber Threats (CT) constructs. As per the rule of thumb, AVE values that are more than 0.50 indicates acceptable convergent validity. However, for the two constructs that did not exceed 0.50, it is still considered valid because the composite reliability values for these two constructs is more than 0.60 (Fornell & David, 1981). Convergent validity is achieved for every constructs. If compared to the original measurement model, convergent validity is not achieved for two of the independent variables constructs.

4.2.1.4 Discriminant Validity

Table 4.3

HTMT Output

	P	O	R	C	AU	CO	RE	FC	CT
P		0.343		0.346	0.369	0.412		0.379	0.330
O				0.050	0.657	0.464		0.746	0.532
R	0.441	0.112		0.825	0.456	0.339		0.153	0.334
C					0.377				
AU									
CO				0.355	0.908				
RE	0.246	0.643	0.186	0.152	0.985	0.684		0.511	0.425
FC				0.179	0.585	0.335			0.751
CT				0.309	0.479	0.345			

The HTMT output shows values for most construct is less than 0.90, which is the acceptable range, except for two; Autonomy (AU) with Competence (CO) and Autonomy (AU) with Relatedness (RE). With this, it can be concluded that the discriminant validity has been established between the constructs.

The above results signify satisfactory values, which indicate our measurement model has achieved an adequate level of reliability and validity (Hair et al., 2014).

4.2.2 Structural Model Assessment

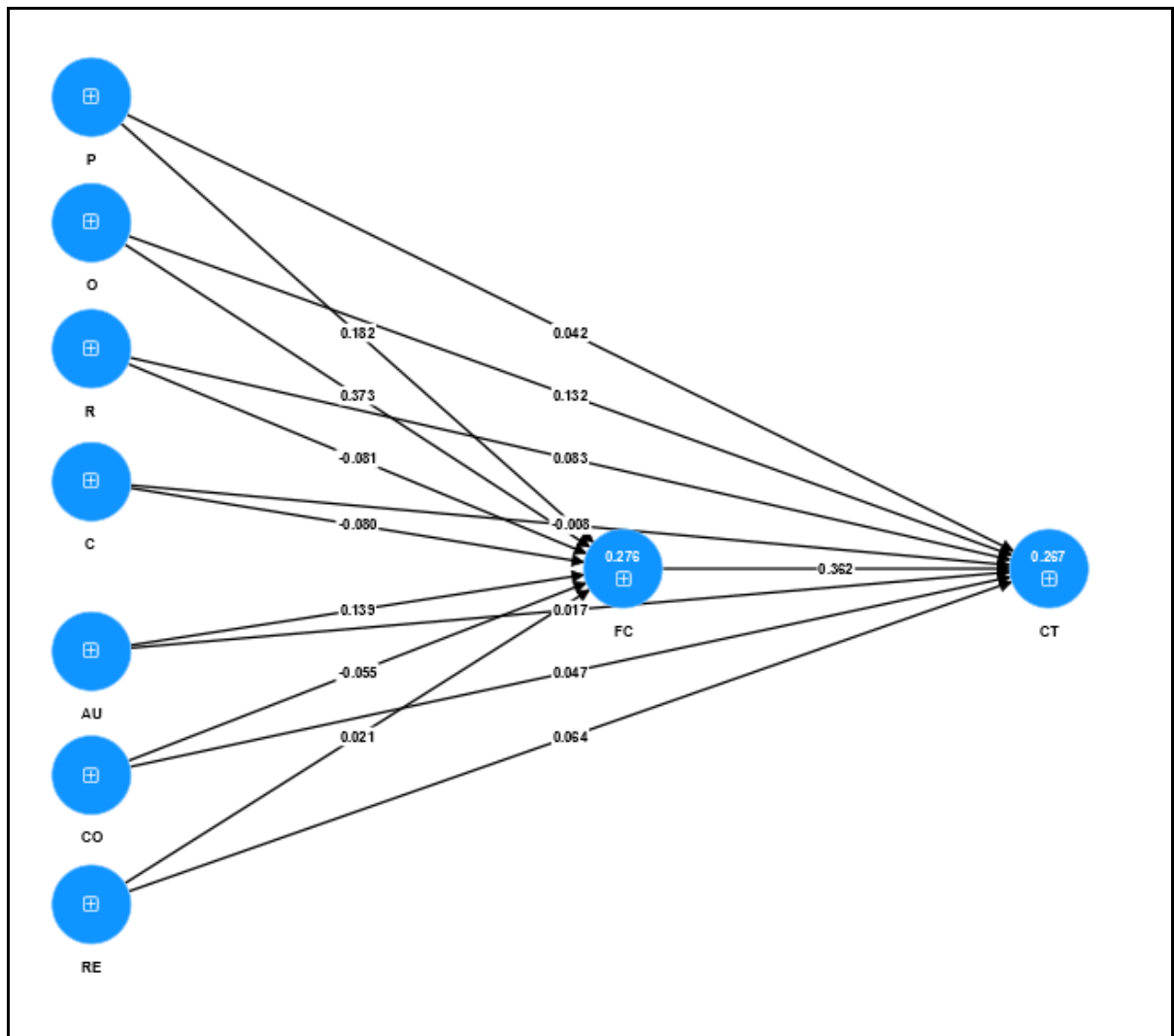


Figure 4.2. Structural Model

4.2.2.1 Collinearity

Table 4.4

Collinearity Results

	P	O	R	C	AU	CO	RE	FC	CT
P								1.253	1.299
O								1.430	1.623
R								1.599	1.608
C								1.730	1.739
AU								2.598	2.625
CO								2.271	2.275
RE								2.354	2.355
FC									1.382
CT									

As the inputs all influence each other, multicollinearity causes a problem in the multiple regression model. It can generate regression coefficient estimates that are not statistically significant. The greater the collinearity, the less reliable the regressions results will be. A collinearity of 1 indicates that the variables are not correlated and that multicollinearity does not present in the regression model (Potters, 2023). Based on the results above, it can be seen that the collinearity among the variables overall shows

values that are less than 5. In other words, there is no occurrence of multicollinearity among the variables.

4.2.2.2 Assess Path Coefficients

Table 4.5

Hypotheses Testing (Path Coefficient, Standard Error, T-Value, p-value and Hypotheses Testing)

Hypotheses	Description	Beta Value	Standard Error	T-Values	P-Value	Decision
H1a	There is a significant relationship between pressure and cyber threats.	0.042	0.070	0.600	0.549	Not supported
H1b	There is a significant relationship between opportunity and cyber threats.	0.132	0.071	1.845	0.065	Not supported
H1c	There is a significant relationship between rationalization and cyber threats.	0.083	0.074	1.117	0.264	Not supported

H1d	There is a significant relationship between capabilities and cyber threats.	-0.008	0.093	0.085	0.932	Not supported
H2a	There is a significant relationship between autonomy and cyber threats.	0.017	0.104	0.162	0.872	Not supported
H2b	There is a significant relationship between competence and cyber threats.	0.047	0.203	0.233	0.816	Not supported
H2c	There is a significant relationship between relatedness and cyber threats.	0.064	0.091	0.698	0.485	Not supported

H1a: "There is a significant relationship between pressure and cyber threats."

Despite the fact that the calculated p-value of 0.549 is greater than the conventional significance level of 0.05, the observed relationship between pressure and cyber threats should not be neglected. The data points to a positive direction in the relationship, indicating that as pressure increases, so may the number of cyber threats. While the

statistical test does not provide enough evidence to support the significance of this relationship, this finding might need further investigation and consideration in a broader context.

H1b: "There is a significant relationship between opportunity and cyber threats."

Although the p-value of 0.065 exceeds the typical significance threshold, the observed positive relationship between opportunity and cyber threats should not be neglected. This implies that there may be a correlation between increased opportunity and a possible rise in cyber threats. While the data does not provide strong evidence of significance, this finding may be useful in understanding potential contributing factors to cyber threats.

H1c: "There is a significant relationship between rationalization and cyber threats."

With a p-value of 0.264, the observed relationship between rationalization and cyber threats does not meet the conventional significance criteria. However, the positive direction of this relationship still suggests that rationalization might play a role in influencing cyber threats. While not statistically significant, this finding could prompt further exploration into the interplay between rationalization and cyber threats.

H1d: "There is a significant relationship between capabilities and cyber threats."

Even though the p-value of 0.932 is far above the significance level, the observed negative relationship between capabilities and cyber threats should be taken into account. This observation raises the question of whether certain capabilities may contribute to a reduction in cyber threats, even though statistical analysis does not support a significant association.

H2a: "There is a significant relationship between autonomy and cyber threats."

While the p-value of 0.872 does not indicate statistical significance, the observed relationship between autonomy and cyber threats may have consequences. According to the data, there is a positive relationship between autonomy and cyber threats, implying that increased autonomy may be associated with an increase in cyber threats.

Although statistical evidence is lacking, this finding may prompt further research into the potential impact of autonomy on cyber threats.

H2b: "There is a significant relationship between competence and cyber threats."

The observed positive relationship between competence and cyber threats might require attention, despite the p-value of 0.816 exceeding the significance threshold. This implies that there may be a link between competence and the occurrence of cyber threats. Although statistical significance is not achieved, this finding may encourage further research into the role of competence in cyber threat dynamics.

H2c: "There is a significant relationship between relatedness and cyber threats."

The observed relationship between relatedness and cyber threats is notable, despite the fact that the p-value of 0.485 does not support statistical significance. This suggests that relatedness may have an impact on cyber threats. Regardless of the lack of statistical support, this finding could lead to further research into the potential impact of relatedness on cyber threat occurrences.

4.2.2.3 Coefficient of Determination (R^2)

Table 4.6

Determination of co-efficient (R^2)

Construct	R^2	R2 Adjusted
CT	0.267	0.251
FC	0.276	0.263

The cyber threats and fraudulent cases are influenced by its independent variables. From the table above, it can be seen that 26.7% of change in dependent variable, Cyber Threats (CT) can be explained the variables. Followed by, 27.6% of changes in mediator, Fraudulent Cases (FC), can be explained by the independent variables.

4.2.2.4 Assess Effect Size f^2

Assessment criteria: small=0.02; medium =0.15; large = 0.35

Table 4.7

Determination of effect size (f^2)

	FC	CT	Effect Size
P	0.036	0.002	Small
O	0.135	0.015	Small
R	0.006	0.006	Small
C	0.005	0.000	Small
AU	0.010	0.000	Small
CO	0.002	0.001	Small
RE	0.000	0.002	Small
FC		0.129	Small

	FC	CT	Effect Size
P	0.036	0.002	Small
O	0.135	0.015	Small
R	0.006	0.006	Small
C	0.005	0.000	Small
CT			

Effect sizes are a useful addition to null hypothesis significance tests like p-values because they provide a measure of practical significance in terms of the magnitude of the effect and are independent of sample size. The effect sizes obtained for all values are less than 0.15, which indicates small effect size.

4.2.2.5 Assess model's predictive relevance (Q^2)

Table 4.8

Determination of predictive relevance (Q^2)

	Original Sample Q^2
P	0.000
O	0.000

R	0.000
C	0.000
AU	0.000
CO	0.000
RE	0.000
FC	0.129
CT	0.100

4.2.2.5 Mediation

Table 4.9

Mediation

Hypothesis	Description	Direct effect (Beta)	t-value	Significance (p<0.05)?	Indirect effect	t-value	Significance (p<0.05)?	Decision
H3	There is a significant relationship between fraudulent cases and cyber threats.	0.362	5.189	0.000				Supported

H3a	Fraudulent cases does mediate the relationship between pressure and cyber threats.	0.108	1.596	0.111	0.066	2.372	0.018	Supported
H3b	Fraudulent cases does mediate the relationship between opportunity and cyber threats.	0.267	3.839	0.000	0.135	3.873	0.000	Supported
H3c	Fraudulent cases does mediate the relationship between rationalization and cyber threats.	0.054	0.694	0.488	-0.029	0.980	0.327	Not supported
H3d	Fraudulent cases does mediate the relationship between capabilities and cyber threats.	-0.037	0.379	0.704	-0.029	0.919	0.358	Not supported
H4a	Fraudulent cases does mediate the relationship between autonomy and cyber threats.	0.067	0.637	0.524	0.050	1.498	0.134	Not supported
H4b	Fraudulent cases does mediate the relationship	0.027	0.135	0.892	-0.020	0.749	0.454	Not supported

	between competence and cyber threats.							
H4c	Fraudulent cases does mediate the relationship between relatedness and cyber threats.	0.071	0.730	0.465	0.008	0.253	0.800	Not supported

H3: “There is a significant relationship between fraudulent cases and cyber threats.”

H3a: “Fraudulent cases does mediate the relationship between pressure and cyber threats.”

H3b: “Fraudulent cases does mediate the relationship between opportunity and cyber threats.”

H3c: “Fraudulent cases does mediate the relationship between rationalization and cyber threats.”

H3d: “Fraudulent cases does mediate the relationship between capabilities and cyber threats.”

The result of testing the mediating effect provide evidence that the relationship between fraudulent cases to cyber threats is statistically significant, thus accepting the alternate hypothesis of H3. The results also shows that fraudulent cases could mediate pressure and opportunity to cyber threats as the values are significant, indicating that the hypothesis is accepted. This proves that due to the pressure and given opportunity, humans can commit fraud which will then lead to increase in fraudulent cases and giving rise to the cyber threats eventually. The other two elements of human factors; H3c and H3d, are not statistically significant.

H4a: Fraudulent cases does mediate the relationship between autonomy and cyber threats.

H4b: Fraudulent cases does mediate the relationship between competence and cyber threats.

H4c: Fraudulent cases does mediate the relationship between relatedness and cyber threats.

The p-values for the above three hypotheses shows that it is statistically not significant. Hence, the alternate hypotheses are not accepted.

As compared to the original model, it shows that the indirect effects for all the hypotheses; H3a, H3b, H3c, H3d, H4a, H4b, H4c, are statistically not significant whereby the p-values are all more than 0.05. This proves that the modified model which is used in our study shows better results in comparison to the original model. (refer Appendix 4.3)

In conclusion, while some of the p-values in this study do not meet the conventional significance threshold, the observed relationships between variables should not be discounted. These findings can provide valuable insight into possible relationships between the factors investigated and cyber threats.

CHAPTER 5: DATA ANALYSIS

5.1 Discussions of Major Findings

Validation of Research Objectives and Hypotheses

The study's key findings provide valuable insights into the factors influencing cyber threats in the financial sector, both from a human and artificial intelligence standpoint. These findings are critical in validating the study's research objectives and hypotheses. Since both studies focus on the subject of fraudulent behavior and cybercrimes, particularly in the context of the banking business, they are consistent with the primary supporting studies in Chapter 2. Both research use theoretical frameworks to better understand the elements that influence fraudulent activity. The Fraud Diamond Theory and Self-Determination Theory are used in our investigation, whereas the mentioned study focuses on the consequences of the Fraud Diamond Theory and AI features. Furthermore, both collect data via questionnaires, reflecting a survey-based strategy to gaining insights from respondents. Furthermore, statistical analysis is used to investigate the correlations between variables. Correlation, regression, and mediation analysis are used in our study, while correlation and regression analyses are used in the context of the research.

The supporting publication, "Artificial Intelligence and Human Psychology in Online Transaction Fraud," is comparable to our work in that it focuses on the relationship between fraudulent conduct, cybercrime, and associated theories. However, significant differences exist between the two studies. Our analysis focuses on Malaysians aged 18 to 55, whereas the referenced publication includes data from 15 Pakistani banks. This implies that several geographical and organizational contexts are involved. While both research assess the implications of Fraud Diamond Theory, we add our analysis with self-determination theory (autonomy, competence, and relatedness). The data was

analyzed using IBM SPSS software in the supporting journal, however SmartPLS software was used in our study.

Research Objective:

1. Understanding Fraud Motivations

The study sought to comprehend the motivations behind cyber threats and fraudulent financial activities. The findings validate this goal by emphasizing the importance of the Fraud Diamond Theory. The theory's components - pressure, opportunity, rationalisation, and capability - have been validated by analyzing various cyber threat cases. The identification of these components in real-world scenarios confirms that fraud frequently occurs as a result of the convergence of these factors. The validation of this objective emphasizes the fact that motivations for cyber threats are rooted in human psychological and situational factors.

2. Reducing the Probability of Becoming a Fraud Victim

The study's findings on the importance of understanding human psychology support the goal of reducing the risk of individuals becoming victims of cyber threats. The study emphasizes the importance of autonomy, competence, and relatedness in influencing individual behavior by delving into the Self-Determination Theory (SDT). According to the findings, understanding these psychological needs can help financial institutions design systems and procedures that reduce vulnerability to cyber threats. The validation of this objective emphasizes the importance of creating an environment that meets employees' and people psychological needs in order to keep them from engaging in fraudulent activities.

Discussion on validation and summary of hypotheses

Although the p-values for some hypotheses did not meet the conventional significance threshold, the observed data trends still provide valuable validation and insights.

Relationships between Pressure, Opportunity, Rationalization, Capabilities and Cyber Threats:

Although the p-values were non-significant, the observed positive directions in these relationships supported the idea that these factors might contribute to cyber threats. The lack of statistical significance implies that these factors may not act independently, but rather interact in complex ways. This is consistent with the Fraud Diamond Theory's comprehensive approach.

Relationships between Autonomy, Competence, Relatedness, and Cyber Threats:

The non-significant p-values cannot be ignored as there are potential impact of these psychological needs on cyber threats. The observed trends suggest that autonomy, competence, and relatedness may influence cyber threats in ways that suggests further investigation. These findings support the goal of learning more about the impact of behavioral requirements on cyber threats.

The study's non-significant findings are critical in validating the research objectives and hypotheses. These findings highlight the complexities of cyber threats and fraud, implying that the motivations and influences driving these activities are complex and interconnected. While statistical significance is an important criterion, the observed trends serve as a foundation for further investigation and future research directions. The study's integrated approach to understanding both human and artificial intelligence factors broaden understanding of cyber threats in the financial sector, validating the overall research objectives.

5.2 Implications of the Study

The research on the Analysis of Human and Artificial Intelligence Influencing Cyber Threats in Malaysian Financial Sectors has significant implications for understanding and mitigating cyber threats in the financial industry. The combination of human behavior and driven by artificial intelligence technologies creates a complex landscape that necessitates comprehensive strategies to effectively address cyber risks. The following are some of the study's implications.

5.2.1 Practical Implications

1. Enhancing Cybersecurity Policies

Financial institutions can improve their fraud detection and prevention mechanisms by better understanding the motivations behind cyber threats, particularly through the application of the Fraud Diamond Theory. Recognising the interplay of perceived pressure, opportunity, rationalisation, and capability can aid in identifying potential vulnerabilities and effectively deterring fraudulent activity. The way Malaysia has handled cyber threats, according to Bank Negara Malaysia, highlights the need for stronger cybersecurity regulations at all levels. The National Cyber Security Framework is critical for protecting critical national information infrastructure (CNII) financial institutions. Regular cyber drills aid in the improvement and adaptation of response programmes to emerging threats. Collaboration is essential for intelligence sharing and best practises among financial institutions, agencies, and the Internet Banking Task Force. IT security is strengthened by defensive strategies, cybersecurity prioritisation, and the Bank's guidelines. Governance, risk assessment, and consumer education all help to build strong plans. Continuous intelligence improvement and coordination are critical components of mitigating cyber risks in the financial sector (Bank Negara Malaysia, 2014).

2. Promoting Cybersecurity Awareness

The study emphasises the critical need for increased cybersecurity awareness among financial sector practitioners. To address this imperative, financial institutions should invest in robust training programmes. These initiatives are intended to educate employees about the multifaceted risks posed by cyber threats and to emphasise the critical importance of adhering to established best practises without fail. Institutions can significantly improve their ability to thwart evolving threats, safeguard sensitive information, and maintain the integrity of the financial sector's operations in an increasingly digital landscape by cultivating a culture of cybersecurity vigilance and knowledge.

This is due to cybercrime has become a major concern for organisations around the world in today's interconnected world. Attacks on businesses have more than doubled in the last five years, necessitating significant investment in comprehensive cybersecurity awareness training by financial institutions. Employees are targeted by various types of fraudulent attacks. Employees unwittingly provide information that leads to over 90% of successful cyber-attacks, making them prime targets. It is critical to develop a security strategy that incorporates cybersecurity into organisational culture in order to raise employee awareness. Training on a regular basis, updating defensive practices, and implementing security awareness programmes are all critical components. These initiatives not only educate employees about cyber threats and data sensitivity, but they also reduce the risk of data breaches and foster a culture of enhanced security compliance. Financial institutions can proactively defend against cyber threats by following these guidelines, ensuring the stability and resilience of their operations (MacKay, 2023).

5.2.2 Theoretical Implications

Fraud Diamond Theory

Pressure (P): None of the correlations between pressure and cyber threats (H1a) or other variables are found to be significant in the hypotheses testing phase. This could imply that perceived non-shareable financial necessity (pressure) is not a good predictor of cyber dangers in the circumstances of the results.

Opportunity (O): Similar to pressure, the connections between opportunity, cyber threats (H1b), and other variables are not significant. This means that, among the listed criteria, the presence of opportunities alone may not be a key driver of cyber hazards.

Rationalization (R): There is no relationship between rationalization and cyber risks (H1c). This suggests that the process of rationalizing dishonest behavior may not be a significant element in explaining cyber dangers in the results.

Capability (C): The relationship between capabilities and cyber threats (H1d) is also insignificant. This shows that, within your specified factors, people's ability to commit fraud may not be highly linked to cyber dangers.

Self-Determination Theory

Autonomy (AU), Competence (CO), Relatedness (RE): Relationships between autonomy, competence, relatedness, and cyber threats (H2a, H2b, H2c) are not significant in the hypothesis testing section. This means that characteristics related to these psychological demands may not be significant factors of cyber dangers among the variables.

Mediator

Fraudulent Cases (FC), According to the mediation analysis section (Table 4.9), fraudulent instances do moderate the relationship between specific characteristics and cyber dangers. This means that as more people engage in fraudulent activities, cyber dangers may increase. This variable of the study is consistent with the Fraud Diamond Theory's concept of perceived opportunity and capacity affecting fraudulent behavior, which could lead to cyber threats.

Significance of the research

The significance of a cybersecurity research study in Malaysia's banking sector. It is significant because of its practical consequences in tackling real-world situations. Malaysia's financial industry is critical to the country's economy and national security, making it a prime target for hackers. Thus, the study emphasis on delivering practical answers and insights into cybersecurity concerns is emphasized. It focuses on the motivations behind cyber fraud, including the human components that motivate fraudsters. It also investigates the role of artificial intelligence (AI) in preventing fraudulent actions. The project intends to provide a comprehensive method to counter cyber dangers by merging insights into human behavior with AI-driven solutions. In addition, governments, financial institutions, and law enforcement agencies are expected to benefit from the development of targeted interventions and preventive measures against cyber fraud. A greater knowledge of human motivations and the capabilities of AI can lead to more effective fraud detection and prevention measures.

Financial institutions' ability to detect fraud is being emphasized as being significantly improved by the use of AI technologies for analyzing massive amounts of data and spotting patterns and abnormalities. Furthermore, the findings can be utilized to educate the public about potential fraud threats. Educating people about cyber hazards enables them to take measures and make educated decisions. Furthermore, it is intended to provide useful insights to future cybersecurity researchers in Malaysia. It offers the framework for future research into topics including human behavior, psychological

factors that encourage fraud, and the efficacy of AI in cyber threat mitigation. It also seeks to understand how fraudulent cases operate as a link between various elements and cyber dangers in Malaysia's banking industry. This knowledge can help lead the development of more effective countermeasures to cyber threats.

1. Policy Makers

Despite the fact that certain correlations were not statistically significant, the observed positive patterns in these relationships suggest possible contributions to cyber risks. Policymakers must acknowledge that the elements bringing about cyber risks may interact in complex ways, and decisions must take these complex relationships into account. Furthermore, the study's integrated approach, which takes into account both human and artificial intelligence components, broadens awareness of cyber dangers in the financial industry. Policymakers should recognize the importance of comprehensive insights that address multiple aspects of cyber dangers, and they can use this information to develop more effective prevention and response plans.

Furthermore, non-significant data are crucial in supporting study aims and hypotheses. They highlight the intricacies of cyber dangers and emphasize the need for additional research. Policymakers should recognize that non-significant conclusions are not failures, but rather stepping stones to greater comprehension. This promotes continuous research and data-driven decision-making. While statistical significance is crucial, observed trends serve as a foundation for future research. Even though they are not statistically verified, these tendencies indicate probable correlations. Policymakers should encourage ongoing research programs that build on these fundamental discoveries. This could include sponsoring more studies or cooperating with researchers to investigate intricate relationships. In addition, statistically significant relationships show the mediation influence of fraudulent cases between certain factors (pressure, opportunity) and cyber dangers. Policymakers must understand the connection between fraudulent acts and eventual cyber dangers. Improving fraud prevention techniques can help to reduce cyber dangers indirectly.

2. Exploration of Human Factors

The study's exploration of human factors and their relationship to cyber threats opens up the possibility to further theoretical investigations. Future research can investigate the psychology of human involvement in cybercrime and look for ways to mitigate these human-centric risks.

Exploration of the human factor in cybersecurity reveals that cybercriminals exploit human vulnerabilities and psychological aspects to gain unauthorised access and steal credentials. This emphasises its importance for Chief Information Security Officers (CISOs), who must consider the human element when protecting against cyber-attacks, especially in the context of human-centric data breaches caused by errors, negligence, and a lack of awareness. However, the negative perception of humans as the weakest link in cybersecurity poses a challenge, impeding discussions about improving their role in cybersecurity processes. While highlighting its significance in fostering a cybersecurity culture, addressing this complex human factor involves nuanced sociological, psychological, and philosophical considerations (Leal, 2022).

3. Comprehensive Cybersecurity Models

Despite not always achieving statistical significance, the study's findings provide an important starting point for the development of comprehensive cybersecurity models. Future research can investigate integrated models that encapsulate the intricate dynamics of cyber threats in the financial sector by acknowledging the interplay between human and artificial intelligence factors. These models can address the study's complicated relationships, paving the way for a comprehensive understanding of motivations, vulnerabilities, and potential safeguards. Incorporating both psychological aspects of individuals and artificial intelligence capabilities, these models can provide a more accurate and effective framework for combating cyber threats, ultimately improving the financial sector's safety precautions.

A collaborative effort including numerous stakeholders with expertise in diverse fields is used to construct comprehensive cybersecurity models. Comprehensive models are conceptualized and created by researchers in fields such as finance, behavioral psychology, cybersecurity, and artificial intelligence. For the models to have a strong base, they can offer theoretical insights and empirical data. Furthermore, experts with knowledge of the financial sector, cybersecurity, and technology can offer useful insights into current issues and recommended practices. Their contribution guarantees the models are suitable, useful, and adaptive to the always-changing threat landscape. Moreover, regulatory bodies in charge of monitoring the financial industry can help by providing standards, compliance requirements, and rules that the comprehensive models should follow. Their participation guarantees that the models adhere to business regulations.

5.3 Limitations of the Study

The limitation of the study is the research gap. This study's research gap relates to its special focus on the fraudulent cases mediating effects on the relationship between human and artificial intelligence factors and cyberthreats in Malaysia's financial sector. There are not numerous in-depth investigations that look at the function of the fraudulent cases as a mediator, but the possibility that prior study may have examined the relationships between these particular factors and cyber threats. Understanding how fraudulent cases affect the relationship between human and artificial intelligence factors and cyber threats might offer important insights into the underlying mechanisms or processes that cause an increase in cyber threats in the financial sector. Moreover, the existing knowledge or information that has not been sufficiently addressed or investigated in prior research with regard to cybersecurity, human and artificial intelligence factors, and cyber threats in the financial sector of Malaysia is referred to as the research gap in this study.

The geographical comparison of East Malaysia to West Malaysia, which is primarily motivated by the higher frequency of fraud cases in East Malaysia, is a fundamental limitation of this study. While using a comparative technique can result in insightful discoveries, there are limitations in terms of generalizability and possible bias. The diversity and complexity of Malaysia's whole financial sector may not be accurately reflected by concentrating only on East and West Malaysia. Furthermore, the human factors, cyber threat environments, and dynamics in other parts of Malaysia could be different from those in the chosen areas. This study may be biased if areas are chosen based on having a greater prevalence of fraud cases. Therefore, this study may be influenced by this bias in ways that may not correctly reflect the overall condition of cyber risks and human factors throughout Malaysia's whole banking sector.

The absence of certain specific job titles, particularly those of Chief Executive Officers (CEOs), is a unique limitation of this research. While this study looks at the relationship between fraud cases, artificial intelligence, and cyberthreats in the financial sector, it may neglect the distinctive viewpoints and decision-making techniques of CEOs, who play the important roles in organizations. A strategic and comprehensive vision of the company is frequently held by CEOs. The direction, risk management, and cybersecurity tactics of the company may all be strongly impacted by their decisions. As a result, this study's inclusion of them could shed light on how senior executives view and respond to the complex interplay of human and artificial intelligence factors, fraudulent cases, and cyberthreats. Compared to other work responsibilities, CEOs may perceive risk differently and may have varied levels of risk tolerance. The role of top-level management in protecting financial institutions can be better understood by gaining an understanding of how CEOs analyze cyber threats, evaluate the effectiveness of security measures, and make decisions regarding fraud prevention.

While investigating fraudulent cases as a mediator variable aids in developing a deeper comprehension of the relationship between factors affecting human and artificial intelligence as well as cyber threats, it's critical to acknowledge the difficulty in establishing clear causality through mediation. The mediation approach presupposes a certain direction of causation, where the mediator, fraudulent cases affects the dependent variable, cyber threats after being influenced by the independent variable, human and artificial intelligence factors. However, causation might not always be straightforward and predictable in complex real-world situations. The mediation relationship may be thrown off if there are unreported or unaccounted for variables. External threats and macroeconomic conditions were not taken into account in the study, but they may have an impact on both fraudulent cases and cyberthreats.

In addition, the limitation of performing the research in a particular area, like Malaysia, is that the results and interpretations may not be as generalizable to other areas or countries. The distinctive traits, cultural context, governing environment, and cybersecurity environment particular to a certain area may have an impact on research undertaken there. When understanding and using the research findings, this limitation needs to be taken into account. Different cultural norms, socioeconomic situations, and technological infrastructures may exist in various nations or areas, and these factors may have an impact on cybersecurity procedures and cyberthreats. As a result, research results obtained from a particular area might not be directly transferable to other locations with differing cultural values and economic circumstances. Moreover, legal and regulatory frameworks for cybersecurity might differ greatly between nations. The cybersecurity laws and regulations that are unique to a given nation, like Malaysia, may have an impact on research done there. These laws and policies may not be compatible with those in other locations. The research results might not apply to areas with various regulatory regimes as a result. While the research may concentrate on Malaysia's financial sector, financial institutions in other nations may employ different cybersecurity procedures, exhibit various degrees of technological expertise, and be more vulnerable to threats.

5.4 Recommendations for Future Research

Researchers should conduct in-depth case studies that concentrate on particular instances of fraud and how they affect the cybersecurity environment to address the identified research gap related to fraudulent cases mediating the relationship between human and artificial intelligence factors and cyberthreats in Malaysia's financial sector. The methods by which fraudulent cases mediate the interaction between human, artificial intelligence, and cyber threat factors can be better understood using this qualitative approach. Furthermore, researchers should attempt to fill this knowledge gap by providing a more comprehensive and integrated understanding of the factors impacting cyber threats in the context of Malaysia's financial sector. The method will provide important direction for policymakers, financial institutions, and cybersecurity practitioners in their efforts to strengthen cybersecurity measures by shedding light on how human and artificial intelligence factors interact with fraudulent cases to impact the likelihood and severity of cyber threats.

Researchers should concentrate on a comparison analysis between East Malaysia and West Malaysia to further enhance the study's conclusions. A statistical comparison of the presence and nature of cyberthreats, human and artificial intelligence variables, and fraudulent cases between these two locations could offer valuable insights given the mention of higher fraud cases in East Malaysia. This strategy might make it easier to spot any regional variances and the possible causes of those changes. This study's findings can help with the establishment of focused cybersecurity strategies by informing policy suggestions that are catered to the unique issues and advantages of each location. Moreover, this study's findings may not only be applicable to Malaysia but also provide greater understanding of how regional differences, cybersecurity, and financial sector behaviour interact.

Researchers should create surveys targeted exclusively at CEOs to gather their opinions on fraud, cyberthreats, and artificial intelligence. Their risk perceptions, decision-making processes, and opinions on the effectiveness of current cybersecurity solutions could all be the subject of questions. For instance, find out what level of risk they connect with cyberattacks, what kind of financial impact they might have, and what they think about how the threat landscape is changing. Furthermore, researchers should create tests that investigate the decisions CEOs make in relation to cybersecurity and fraud avoidance. Researchers should examine the variables that affect their decisions, such as technological viability, financial ramifications, and regulatory compliance. Researchers should find out if they anticipate the need for increased security in the future and whether they think the cybersecurity measures in place at their company are acceptable.

Researchers should conduct sensitivity analyses to evaluate the mediation model's robustness under various situations and suppositions. Sensitivity analyses examine the stability of the mediation model's results under various scenarios, assumptions, and parameters. Researchers can find out if their findings hold under many circumstances by evaluating the robustness of the model. Researchers can explore the effects of various assumptions on the results of the mediation model using sensitivity analyses. This ensures that the results are not overly dependent on certain presumptions. Furthermore, control variables are used to take into account the impact of external factors that might affect the relationship between the mediator, fraudulent cases and the dependent variable, cyber threats. Researchers intend to isolate the specific impact of the mediator and reduce the chance of making incorrect assumptions by introducing control variables. This can make it easier to separate the impact of fraudulent cases and give a more precise assessment of their mediating function.

Researchers should apply a multi-dimensional strategy that considers the cultural, social, technological, and regulatory settings of the investigated location in order to

solve the constraint of generalizability caused by conducting research in a particular place, such as Malaysia. Researchers can work with specialists from different nations and international institutions to learn more about cybersecurity practices and cyberthreats in diverse regions. The study's scope can be widened, and a variety of viewpoints can be guaranteed in this way. Comparative studies can be created by researchers to look at cybersecurity procedures and cyberthreats in various nations or regions. The research findings may be more broadly applicable by examining similarities and differences. Assess the consistency of results across regions by doing the research again in other geographic contexts. As a result, the variances that might occur and the generalizability of the findings are more well understood. The context of the study region should be explicitly acknowledged when interpreting the research findings, and it should be emphasized that the findings are applicable in that particular setting. Moreover, work together with researchers from various geographical areas to include a range of viewpoints and experiences, which can enrich the richness of the study's findings. The limitations of the research location should be acknowledged in the study's conclusions, and it should be made apparent that the results are unique to the chosen location. They must refrain from drawing conclusions outside the parameters of their research.

REFERENCES

- Abdullahi, R., & Mansor, N. (2018). Fraud prevention initiatives in the Nigerian public sector: understanding the relationship of fraud incidences and the elements of fraud triangle theory. *Journal of Financial Crime*.
- Ackerman, C. E. (2018, June 21). *Self Determination Theory and How It Explains Motivation*. Retrieved from Motivation & Goals: <https://positivepsychology.com/self-determination-theory/>
- Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, 8, 137293-137311.
- Anand, A. (2021, September 21). *How is AI used in Fraud Detection?* Retrieved from analyticSteps: <https://analyticsteps.com/blogs/how-ai-used-fraud-detection>
- Avortri, C., & Agbanyo, R. (2020). Determinants of management fraud in the banking sector of Ghana: the perspective of the diamond fraud theory. *Journal of Financial Crime*, 28(1), 142-155.
- Bank Negara Malaysia. (2021). Annual Report 2020. Retrieved from <https://www.bnm.gov.my/-/annual-report-2020>
- Birruntha, S. (2023, May 15). Three out of five Malaysians willing to commit fraud to obtain loans, file insurance claims: FICO study. New Straits Times. Retrieved from <https://www.nst.com.my/business/2023/05/909591/three-out-five-malaysians-willing-commit-fraud-obtain-loans-file-insurance>
- Ching Sing Chai, T. K.-F. (2020). Modeling Chinese Secondary School Students' Behavioral Intentions to Learn Artificial Intelligence with the Theory of Planned Behavior and Self-Determination Theory. *sustainability*, 16.
- Cherry, K. (2022, November 8). How does self-determination theory explain motivation? Verywell Mind.

- Crowther, D., & Lancaster, G. (2012). *Research methods*. Routledge.
- Diansari, R. E., & Wijaya, A. T. (2019). Diamond fraud analysis in detecting financial statement fraud. *Journal of Business and Information Systems (e-ISSN: 2685-2543)*, 1(2), 63-76.
- Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in accounting education*, 27(2), 555-579.
- Firdaus, R., Xue, Y., Gang, L., & e Ali, M. S. (2022). Artificial Intelligence and Human Psychology in Online Transaction Fraud. *Frontiers in Psychology*, 13.
- Frendy, 2022. Examining the fraud diamond theory through ethical culture variables: A study of regional development banks in Indonesia. Taylor & Francis. Retrieved from <https://www.tandfonline.com/doi/full/10.1080/23311975.2022.2117161>
- Fornell, C. & Larcker, D. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research* Vol. 18, No. 1 (Feb), pp. 39-50.
- Guthrie, C., Fosso-Wamba, S., & Arnaud, J. B. (2021). Online consumer resilience during a pandemic: An exploratory study of e-commerce behavior before, during and after a COVID-19 lockdown. *Journal of Retailing and Consumer Services*, 61, 102570.
- In J. (2017). Introduction of a pilot study. *Korean journal of anesthesiology*, 70(6), 601–605. <https://doi.org/10.4097/kjae.2017.70.6.601>
- Jiang, R. (2022). Exploring Employees' Computer Fraud Behaviors using the Fraud Triangle Theory. *Pacific Asia Journal of the Association for Information Systems*, 14(4), 4.

- Kazemian, S., Said, J., Nia, E. H., & Vakilifard, H. (2019). Examining fraud risk factors on asset misappropriation: Evidence from the Iranian banking industry. *Journal of Financial Crime*. <https://doi.org/10.1108/JFC-01-2018-0008>
- Khairuddin, A. M., Yusof, N. A., Ramly, N. A., Hassan, N. A., & Bahari, S. H. (2020). A study on cyber threats in financial institutions in Malaysia. *Journal of Critical Reviews*, 7(8), 107-114.
- Kim Cocks, D. J. (2013). Sample size calculations for pilot randomized trials: a confidence interval approach. *Journal Clinical Epidemiology*, 5.
- Krejcie, R.V., & Morgan, D.W., (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*.
- Leal, A. (2022, August 15). Human factor in cybersecurity: The weakest link?. KuppingerCole. <https://www.kuppingercole.com/events/csIs2022/blog/human-factor-in-cybersecurity-the-weakest-link>
- Malaysia, D. o. (2022, November 29). *CRIME STATISTICS, MALAYSIA, 2022*. Retrieved from Department of Statistics Malaysia Official Portal: [https://www.dosm.gov.my/v1/index.php?r=column/cthemByCat&cat=455&bul_id=RnBiQjA1VHhmelZRVCszS3RiRXpNQT09&menu_id=U3VPMldoYUxzVzFaYmNkWXZteGduZz09#:~:text=Fraud%20cases%20were%20the%20highest,money%20cases%20\(204%20cases\)](https://www.dosm.gov.my/v1/index.php?r=column/cthemByCat&cat=455&bul_id=RnBiQjA1VHhmelZRVCszS3RiRXpNQT09&menu_id=U3VPMldoYUxzVzFaYmNkWXZteGduZz09#:~:text=Fraud%20cases%20were%20the%20highest,money%20cases%20(204%20cases)).
- Ma, K. W. F., & McKinnon, T. (2022). COVID-19 and cyber fraud: emerging threats during the pandemic. *Journal of Financial Crime*, 29(2), 433-446.
- Mangala, D., & Soni, D. (2022). A systematic literature review on frauds in banking sector, *Journal of Financial Crime*. <https://doi.org/10.1108/JFC-12-2021-0263>
- Maulidi, A. (2020). When and why (honest) people commit fraudulent behaviours? Extending the fraud triangle as a predictor of fraudulent behaviours. *Journal of Financial Crime*, 27(2), 541-559.

- MacKay, J. (2023, March 9). How to promote Cyber Security Awareness in your organisation. MetaCompliance. <https://www.metacompliance.com/blog/cyber-security-awareness/how-to-promote-cyber-security>
- Mardhiah, A. (2023, January 11). Ramp up security amid rise of financial fraud. The Malaysian Reserve. Retrieved from <https://themalaysianreserve.com/2023/01/11/ramp-up-security-amid-rise-of-financial-fraud/>
- Mishra, S. (2023, May 10). Exploring the impact of AI-based Cyber Security Financial Sector Management. MDPI. <https://www.mdpi.com/2076-3417/13/10/5875>
- Mukherjee, S., Mukherjee, S., & Guo, Y. (2020). Cybersecurity of internet of things in financial services industry: A review of risks and challenges. *Journal of Financial Crime*, 27(4), 1004-1026.
- Netemeyer, R. et. al. (2003). *Scaling Procedure: Issues and Applications*. SAGE
- Nikolopoulou, K. (2022, August 9). What is convenience sampling? Retrieved from <https://www.scribbr.com/methodology/convenience-sampling/#:~:text=Convenience%20sampling%20is%20a%20non,to%20participate%20in%20the%20research.>
- Nor, N. M., Yusof, R., Bakar, N. A., & Alias, N. A. (2020). Enhancing cybersecurity preparedness in the Malaysian financial industry: A proposed cyber risk management framework. *International Journal of Supply Chain Management*, 9(1), 901-910.
- Potters, C. (2023, February 12). Variance Inflation Factor. <https://www.investopedia.com/terms/v/variance-inflation-factor.asp>
- Qi Xia, T. K. (2022). A self-determination theory (SDT) design approach for inclusive and diverse artificial intelligence (AI) education. *Computers & Education*, 13.

- Romanchuk, J. (2023, March 6). The four types of research design. Retrieved from <https://blog.hubspot.com/marketing/types-of-research-design#:~:text=There%20are%20four%20common%20types,%2C%20experimental%2C%20and%20diagnostic%20designs.>
- Satar, D. S. A. (2019, October 29). Corruption among youths. *New Straits Times*. Retrieved from <https://www.nst.com.my/opinion/columnists/2019/10/533939/corruption-among-youths>
- Sunardi, S., & Amin, M. N. (2018). Fraud detection of financial statement by using fraud diamond perspective. *International Journal of Development and Sustainability*, 7(3), 878-891.
- Taber, K.S. The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Res Sci Educ* 48, 1273–1296 (2018). <https://doi.org/10.1007/s11165-016-9602-2>
- Tunggal, A. T. (2022, August 17). *What is a Cyber Threat?* From UpGuard: <https://www.upguard.com/blog/cyber-threat#:~:text=Cyber%20threats%20include%20computer%20viruses,attacks%2C%20and%20other%20attack%20vectors.>
- Vousinas, G. (2018). Elaborating on the theory of fraud. New theoretical extensions. *New Theoretical Extensions (April 16, 2018)*.
- Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: a systematic mapping of literature. *IEEE Access*, 8, 146598-146612.
- Wolfe, D. T. & Hermanson, D. R. (2004). "The Fraud Diamond: Considering the Four Elements of Fraud." *CPA Journal* 74.12 (2004): 38-42

Xia, Q., Chiu, T. K., Lee, M., Sanusi, I. T., Dai, Y., & Chai, C. S. (2022). A self-determination theory (SDT) design approach for inclusive and diverse artificial intelligence (AI) education. *Computers & Education*, 189, 104582.

APPENDICES

Appendix 3.1: Questionnaire

SECTION A: Demographic

1. Gender

- Male
- Female

2. Age

- 18-25 years old
- 26-30 years old
- 31-40 years old
- 41-50 years old
- 51-55 years old

3. Academic qualification

- SPM/ Certification
- Diploma
- Bachelor's Degree
- Masters/ Doctorate

4. Current position / Work designation

- Unemployed
- Top management
- Middle management
- Supervisor
- Support Staff
- Others

5. Monthly income

- Less than RM999
- RM1000 – RM2999

- RM 3000 – RM4999
- RM5000 and above

6. Number of years of work experience

- Less than 1 year
- 1-5 years
- 6-10 years
- 10 years and above

INSTRUCTIONS

Below there are 27 statements with which you may agree or disagree. There are five ratings on the scale, with 1 being the lowest whereas 5 being the highest. Please indicate your agreement for each statement on the scale of 1-5 by selecting the option beside each statement.

SECTION B:

Cyber Threats (Human and artificial intelligence factors influencing the cyber threats)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
1. My vulnerability to cyber threats is unaffected by my personal factors.	1	2	3	4	5
2. My workplace's culture, rules and operations are	1	2	3	4	5

influenced by cyber threats.					
3. Artificial intelligence strives to lessen the financial sector penetration and instruction and software fraud.	1	2	3	4	5
4. In a constantly shifting world, artificial intelligence does not assist in identifying rapid solutions.	1	2	3	4	5

Questions on cyber threats. Adapted from Kazemian, S., Said, J., Nia, E. H., & Vakilifard, H. (2019). Examining fraud risk factors on asset misappropriation: evidence from the Iranian banking industry. *Journal of Financial Crime*, 26(2), 447-463 and from Salameh, R., & Lutfi, K. (2021). The role of artificial intelligence on limiting Jordanian commercial banks cybercrimes. *Accounting*, 7(5), 1147-1156.

SECTION C:

Human Factors

Pressure (People may commit fraud due to pressure from both financial and non-financial sources)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
1. I am unable to cover my monthly expenses.	1	2	3	4	5
2. I have unexpected financial needs.	1	2	3	4	5
3. I feel depressed due to my excessive workload.	1	2	3	4	5
4. I have a great deal of debt to pay off.	1	2	3	4	5

Opportunity (Opportunity can be used to explain a person’s willingness to commit fraud when there is a chance to do so)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
5. My workplace’s transactions are sufficiently stringent	1	2	3	4	5

and have proper documentation.					
6. My workplace's closed-circuit television (CCTV) monitoring of entrances and exits is adequate.	1	2	3	4	5

Rationalization (Justification for the action of someone committing fraud is called rationalization)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
7. If I use my company's money or resources for personal gain, no one will be harmed.	1	2	3	4	5
8. I believe the company will go bankrupt if I steal a little money from them.	1	2	3	4	5

Capabilities (The ability of a person to commit fraud and their position within an organization are determined by their capabilities)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
9. I am able to misuse the resources at my workplace given my influence over a specific situation.	1	2	3	4	5
10. If I have a higher position at my workplace, I will commit fraud.	1	2	3	4	5

Questions on human factors. Adapted from Kazemian, S., Said, J., Hady Nia, E., & Vakilifard, H. (2019). Examining fraud risk factors on asset misappropriation: evidence from the Iranian banking industry. *Journal of Financial Crime*, 26(2), 447-463 and from Dwi Ratmono & Frendy (2022) Examining the fraud diamond theory through ethical culture variables: A study of regional development banks in Indonesia, *Cogent Business & Management*, 9:1, DOI: 10.1080/23311975.2022.2117161

Artificial Intelligence Factors

Autonomy (Individual's choice in learning artificial intelligence)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
11. I have the right to decide what artificial intelligence skills I would like to learn.	1	2	3	4	5
12. I can have my own choice in what I choose to learn about artificial intelligence skills that I think would benefit me.	1	2	3	4	5
13. I should not voice out my opinions on artificial intelligence as I learn more about it.	1	2	3	4	5
14. I am not afraid to speak my mind when it comes to concerns I have about artificial intelligence learning.	1	2	3	4	5

Competence (Facilitating learning in artificial intelligence)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
15. I feel more confident when I learn more about artificial intelligence.	1	2	3	4	5
16. Learning about artificial intelligence makes me feel like I am able to understand the current trend of AI technology.	1	2	3	4	5
17. It would be challenging for me to understand AI technology.	1	2	3	4	5
18. I feel like it is difficult for me to master AI technology.	1	2	3	4	5

Relatedness (Interpersonal involvement in artificial intelligence)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
19. I believe that studying about artificial intelligence will be relevant in my life.	1	2	3	4	5
20. I can relate more to the current technology when I learn about artificial intelligence.	1	2	3	4	5

Questions on artificial intelligence factors. Adapted from Xia, Q., Chiu, T. K., Lee, M., Sanusi, I. T., Dai, Y., & Chai, C. S. (2022). A self-determination theory (SDT) design approach for inclusive and diverse artificial intelligence (AI) education. *Computers & Education, 189*, 104582 and from Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2021). Adoption of artificial intelligence in banking services: an empirical analysis. *International Journal of Emerging Markets*, (ahead-of-print).

SECTION D:

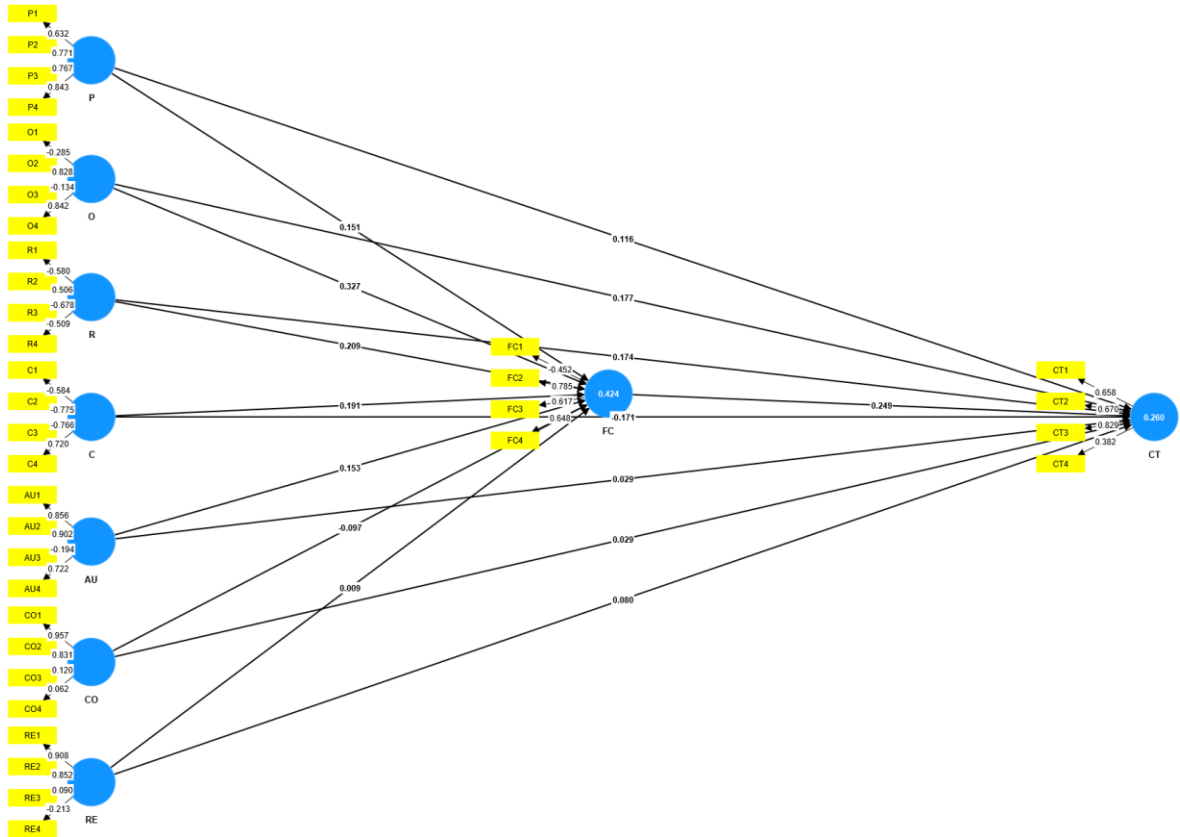
Fraudulent Cases (Impacts of human and artificial intelligence factors on fraudulent cases)

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree

1. I never utilize my workplace's internet service for any personal or illegal activities.	1	2	3	4	5
2. I think using artificial intelligence puts my privacy at stake.	1	2	3	4	5
3. Utilizing artificial intelligence does not expose my account to fraud.	1	2	3	4	5

Questions on fraudulent cases. Adapted from Kazemian, S., Said, J., Hady Nia, E., & Vakilifard, H. (2019). Examining fraud risk factors on asset misappropriation: evidence from the Iranian banking industry. *Journal of Financial Crime*, 26(2), 447-463 and from Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2021). Adoption of artificial intelligence in banking services: an empirical analysis. *International Journal of Emerging Markets*, (ahead-of-print).

Appendix 4.1: Original Measurement Model



Appendix 4.2: Original Reliability Statistics and Validity

Construct reliability and validity - Overview Zoom (80%) Copy to Excel Copy to R

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
AU	0.608	0.762	0.734	0.526
C	0.589	0.729	0.502	0.511
CO	0.721	0.755	0.621	0.406
CT	0.587	0.627	0.738	0.429
FC	0.330	0.510	0.518	0.405
O	0.546	0.562	0.384	0.373
P	0.791	0.740	0.842	0.573
R	0.627	0.103	0.372	0.328
RE	0.437	0.724	0.528	0.401

Appendix 4.3: Original Specific Indirect Effects and Total Indirect Effects

Specific indirect effects - Mean, STDEV, T values, p values Zoom (80%) Copy to Excel

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
C -> FC -> CT	0.048	0.047	0.034	1.413	0.158
R -> FC -> CT	0.052	0.033	0.041	1.262	0.207
AU -> FC -> CT	0.038	0.034	0.033	1.141	0.254
CO -> FC -> CT	-0.024	-0.004	0.029	0.845	0.398
P -> FC -> CT	0.038	0.042	0.026	1.427	0.154
O -> FC -> CT	0.082	0.089	0.043	1.896	0.058
RE -> FC -> CT	0.002	0.010	0.033	0.067	0.946

Total indirect effects - Mean, STDEV, T values, p values Zoom (80%) Copy to Excel

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
AU -> CT	0.038	0.034	0.033	1.141	0.254
C -> CT	0.048	0.047	0.034	1.413	0.158
CO -> CT	-0.024	-0.004	0.029	0.845	0.398
O -> CT	0.082	0.089	0.043	1.896	0.058
P -> CT	0.038	0.042	0.026	1.427	0.154
R -> CT	0.052	0.033	0.041	1.262	0.207
RE -> CT	0.002	0.010	0.033	0.067	0.946

Appendix 4.4: Reliability Statistics and Validity (*used in this study*)

Construct reliability and validity - Overview Zoom (80%)

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
AU	0.608	0.804	0.758	0.533
C	0.830	1.022	0.917	0.846
CO	0.721	0.893	0.642	0.414
CT	0.587	0.619	0.750	0.437
FC	0.563	0.566	0.775	0.535
O	0.708	0.714	0.872	0.774
P	0.791	0.795	0.849	0.586
R	0.636	0.651	0.845	0.732
RE	0.731	0.731	0.881	0.788

Appendix 4.5: HTMT Output (*used in this study*)

Discriminant validity - Heterotrait-monotrait ratio (HTMT)

	AU	C	CO	CT	FC	O	P	R	RE
AU									
C	0.377								
CO	0.908	0.355							
CT	0.479	0.309	0.345						
FC	0.585	0.179	0.335	0.751					
O	0.657	0.050	0.464	0.532	0.746				
P	0.369	0.346	0.412	0.330	0.379	0.343			
R	0.456	0.825	0.339	0.334	0.153	0.112	0.441		
RE	0.985	0.152	0.684	0.425	0.511	0.643	0.246	0.186	

Appendix 4.6: Collinearity (*used in this study*)

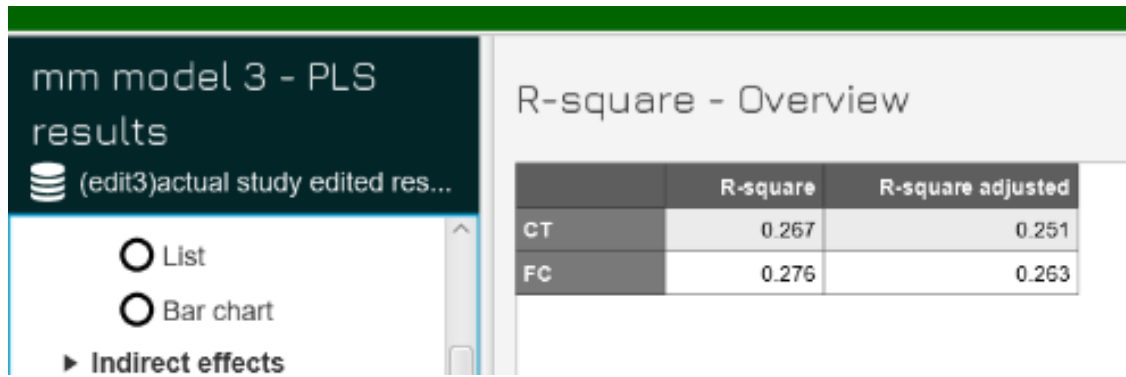
Collinearity statistics (VIF) - Inner model - Matrix

	AU	C	CO	CT	FC	O	P	R	RE
AU				2.625	2.598				
C				1.739	1.730				
CO				2.275	2.271				
CT									
FC				1.382					
O				1.623	1.430				
P				1.299	1.253				
R				1.608	1.599				
RE				2.355	2.354				


Appendix 4.7: Path Coefficients (*used in this study*)

Path coefficients - Mean, STDEV, T values, p values Zoom (80%)

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
AU → CT	0.017	0.028	0.104	0.162	0.872
AU → FC	0.139	0.137	0.086	1.628	0.104
C → CT	-0.008	0.028	0.093	0.085	0.932
C → FC	-0.080	-0.069	0.080	1.003	0.315
CO → CT	0.047	-0.019	0.203	0.233	0.816
CO → FC	-0.055	-0.028	0.072	0.766	0.444
FC → CT	0.362	0.361	0.070	5.189	0.000
O → CT	0.132	0.132	0.071	1.845	0.065
O → FC	0.373	0.374	0.062	6.037	0.000
P → CT	0.042	0.049	0.070	0.600	0.549
P → FC	0.182	0.184	0.066	2.772	0.006
R → CT	0.083	0.094	0.074	1.117	0.264
R → FC	-0.081	-0.089	0.086	0.944	0.345
RE → CT	0.064	0.062	0.091	0.698	0.485
RE → FC	0.021	0.006	0.080	0.261	0.794

Appendix 4.8: R Square (*used in this study*)

Appendix 4.9: f square (used in this study)

f-square - Matrix Zoort 

	AU	C	CO	CT	FC	O	P	R	RE
AU				0.000	0.010				
C				0.000	0.005				
CO				0.001	0.002				
CT									
FC				0.129					
O				0.015	0.135				
P				0.002	0.036				
R				0.006	0.006				
RE				0.002	0.000				

Appendix 4.10: Specific Indirect Effects and Total Indirect Effects (*used in this study*)

Specific indirect effects - Mean, STDEV, T values, p values Zoom (80%)

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
C -> FC -> CT	-0.029	-0.027	0.032	0.919	0.358
R -> FC -> CT	-0.029	-0.030	0.030	0.980	0.327
AU -> FC -> CT	0.050	0.050	0.034	1.498	0.134
CO -> FC -> CT	-0.020	-0.010	0.027	0.749	0.454
P -> FC -> CT	0.066	0.067	0.028	2.372	0.018
O -> FC -> CT	0.135	0.135	0.035	3.873	0.000
RE -> FC -> CT	0.008	0.003	0.030	0.253	0.800

Total indirect effects - Mean, STDEV, T values, p values Zoom (80%)

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
AU -> CT	0.050	0.050	0.034	1.498	0.134
C -> CT	-0.029	-0.027	0.032	0.919	0.358
CO -> CT	-0.020	-0.010	0.027	0.749	0.454
O -> CT	0.135	0.135	0.035	3.873	0.000
P -> CT	0.066	0.067	0.028	2.372	0.018
R -> CT	-0.029	-0.030	0.030	0.980	0.327
RE -> CT	0.008	0.003	0.030	0.253	0.800

Appendix 4.11: Total Effects (*used in this study*)

Total effects - Mean, STDEV, T values, p values Zoom (80%)

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
AU -> CT	0.067	0.078	0.106	0.637	0.524
AU -> FC	0.139	0.137	0.086	1.628	0.104
C -> CT	-0.037	0.001	0.097	0.379	0.704
C -> FC	-0.080	-0.069	0.080	1.003	0.316
CO -> CT	0.027	-0.030	0.203	0.135	0.892
CO -> FC	-0.055	-0.028	0.072	0.766	0.444
FC -> CT	0.362	0.361	0.070	5.189	0.000
O -> CT	0.267	0.267	0.070	3.839	0.000
O -> FC	0.373	0.374	0.062	6.037	0.000
P -> CT	0.108	0.116	0.067	1.596	0.111
P -> FC	0.182	0.184	0.066	2.772	0.006
R -> CT	0.054	0.064	0.077	0.694	0.488
R -> FC	-0.081	-0.089	0.086	0.944	0.345
RE -> CT	0.071	0.065	0.097	0.730	0.465
RE -> FC	0.021	0.006	0.080	0.261	0.794