UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Faculty of Technology Management and Technopreneurship

EXPLORING INSIDER THREATS USING ORGANISATIONAL PERFORMANCE FRAMEWORK IN MALAYSIAN MANUFACTURING CASE

Siti Norfatihah Binti Isnin

Doctor of Philosophy

2024

EXPLORING INSIDER THREATS USING ORGANISATIONAL PERFORMANCE FRAMEWORK IN MALAYSIAN MANUFACTURING CASE

SITI NORFATIHAH BINTI ISNIN

A thesis submitted
in fulfilment of the requirements for the degree of Doctor of Philosophy

Faculty of Technology Management and Technopreneurship

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2024

DEDICATION

In the name of God, the Most Gracious, the Most Merciful. SubhanAllah, AllahuAkhbar, Alhamdulillah for everything. Till now, I still can’t believe I am completed this journey to the end. To my beloved family members; Husband - Amirrudin bin Yaacob, Grandmother - Zaipah Surin, Parents - Fatimah Kassim and Isnin Aman, Kids - Muhammad Fakhruddin Athar, Muhammad Falahuddin Amzar and Nur Faiha Aisyah, Parents in law - Jamaliah Said, Yaacob Dewa, Siblings – Fais Syu, Faiszah Qucai Yusof, Faiszudin, Faiszam, and to all my sister in laws – Ita, Ija, Ida, Nani, Ijan, Ecah and their family members who always support me with du’a, smiles and hugs. Special thanks to Associate Professor Dr. Muliati Sedek and Professor Ts. Dr. Rabiah Ahmad. No matter how challenging *the situation, these are the person who never gives up, always supporting, giving time and keeps praying until I succeed and finish my doctorate journey. Yes, I am Ph.D. survival. It is not an easy journey for me.* **If all difficulties were known at the outset of a long journey, most of us would never start out at all.**

ABSTRACT

The threats that insiders pose to businesses, institutions, and governmental organisations continue to be of serious concern. Recent industry surveys and academic literature provide unequivocal evidence to support the significance of this threat and its prevalence. Mitigating insider threats is a challenging task, which may have been the biggest problem for most organisations without them realising it. Henceforth, this study gauged the employees' agreement level toward the recommended practices to mitigate insider threats by understanding the characteristics of potential insider threats and their impact on organisational performance. The recommended practices were derived from the Common-Sense Guide to Understanding the Characteristics of Insider Threats guide produced by CMU-CERT – Carnegie Melon University, Computer Emergency Response Team. It offers an effective, possible approach from identifying to understanding cerinsider threats and a framework for characterising the attacks. Inspired from the guide, this study suggests the Characterising Insider Threat as the on-going and cyclic processes to deter and detect potential employees bound to become fraudsters or perpetrators in violating the access and trust given by the employer that will impact organisational performance. Validation of the proposed framework was conducted through a triangualtion method, combining distributed questionnaires to respondents and surveys with in-depth interviews and small-group discussions involving three expert panels from Malaysia's manufacturing industry. This triangulation method, augmented by a semi-qualitative approach, facilitated a nuanced exploration of employees' perceptions and experiences regarding insider threats and the effectiveness of recommended mitigation practices. Analysis of data collected from 352 respondents underscored the importance of recognising and addressing six critical factors—Psychological State, Personality Characteristics, Historical Behavior, Motivation to Attack, Skill Set and Opportunity, and the role of Precipitating Events—as essential components of an effective insider threat mitigation strategy. The findings suggest that organisational efforts to identify and suppress these factors can play a pivotal role in mitigating the risk of insider threats and safeguarding organisational reputation and performance. In conclusion, this study offers valuable insights into the acceptance of recommended practices for mitigating insider threats and highlights the importance of organisational vigilance and resilience. By leveraging the proposed framework and insights from industry experts, organizations can enhance their capacity to identify, deter, and respond to insider threats effectively, thereby fostering a culture of trust and accountability conducive to sustained success.

PENEROKAAN ANCAMAN DALAM MENGGUNAKAN RANGKA KERJA PRESTASI ORGANISASI DALAM KES PEMBUATAN MALAYSIA

ABSTRAK

Ancaman yang ditimbulkan oleh orang dalam kepada perniagaan, institusi dan organisasi kerajaan terus menjadi perhatian serius. Tinjauan industri dan literatur akademik terkini memberikan bukti yang jelas untuk menyokong kepentingan ancaman ini dan kelazimannya. Mengurangkan ancaman orang dalam ialah tugas yang mencabar, yang mungkin menjadi masalah terbesar bagi kebanyakan organisasi tanpa mereka sedari. Selepas itu, kajian ini mengukur tahap persetujuan pekerja terhadap amalan yang disyorkan untuk mengurangkan ancaman orang dalam dengan memahami ciri-ciri potensi ancaman orang dalam dan kesannya terhadap prestasi organisasi. Amalan yang disyorkan diperolehi daripada Panduan Akal Waras untuk Memahami Ciri-ciri Ancaman Orang Dalam yang dihasilkan oleh CMU-CERT - Universiti Carnegie Melon, Pasukan Tindak Balas Kecemasan Komputer. Ia menawarkan pendekatan yang berkesan dan mungkin daripada mengenal pasti kepada memahami ancaman cerinsider dan rangka kerja untuk mencirikan serangan. Diilhamkan daripada panduan tersebut, kajian ini mencadangkan Mencirikan Ancaman Orang Dalam sebagai proses berterusan dan kitaran untuk menghalang dan mengesan pekerja berpotensi yang terikat untuk menjadi penipu atau pelaku dalam melanggar akses dan kepercayaan yang diberikan oleh majikan yang akan memberi kesan kepada prestasi organisasi. Pengesahan rangka kerja yang dicadangkan telah dijalankan melalui kaedah triangual, menggabungkan soal selidik yang diedarkan kepada responden dan tinjauan dengan temu bual mendalam dan perbincangan kumpulan kecil yang melibatkan tiga panel pakar dari industri pembuatan Malaysia. Kaedah triangulasi ini, ditambah dengan pendekatan separa kualitatif, memudahkan penerokaan bernuansa persepsi dan pengalaman pekerja berkenaan ancaman orang dalam dan keberkesanan amalan mitigasi yang disyorkan. Analisis data yang dikumpul daripada 352 responden menggariskan kepentingan mengenali dan menangani enam faktor kritikal—Keadaan Psikologi, Ciri Personaliti, Tingkah Laku Sejarah, Motivasi untuk Menyerang, Set Kemahiran dan Peluang, dan Peranan eristiwa Mencetuskan—sebagai komponen penting orang dalam yang berkesan. strategi mitigasi ancaman. Penemuan menunjukkan bahawa usaha organisasi untuk mengenal pasti dan menyekat faktor-faktor ini boleh memainkan peranan penting dalam mengurangkan risiko ancaman orang dalam dan menjaga reputasi dan prestasi organisasi. Kesimpulannya, kajian ini menawarkan pandangan berharga tentang penerimaan amalan yang disyorkan untuk mengurangkan ancaman orang dalam dan menyerlahkan kepentingan kewaspadaan dan daya tahan organisasi. Dengan memanfaatkan rangka kerja dan pandangan yang dicadangkan daripada pakar industri, organisasi boleh meningkatkan keupayaan mereka untuk mengenal pasti, menghalang dan bertindak balas terhadap ancaman orang dalam dengan berkesan, sekali gus memupuk budaya amanah dan akauntabiliti yang kondusif untuk kejayaan yang berterusan.

ACKNOWLEDGEMENTS

Alhamdulillahi rabbil 'alamin. Praise Allah (SWT) the Almighty for the successful completion of this thesis. This very challenging journey in the pursuit of my Ph.D. study has finally reached its destination. I could never do this alone without the support of loving people around me.

I wish to convey my utmost gratitude to Associate Professor Dr. Muliati Sedek for her supervision, care, support, tolerance, and encouragement throughout all these though years. Academically, she always provides me constructive and insightful advice for my research work. My special thanks are also to my second supervisor, Associate Professor Dr. Norfaridatul Akmaliah Othman, for supporting me to finish this thesis. Professor Ts. Dr. Rabiah Ahmad always helped me publish my research with helpful comments, support, and understanding.

My sincere thanks also go to dear FPTT and UTeM's staff who helped me a lot during my study duration. I want to say thank you so much for your understanding and always support and motivate me when I feel down during the Ph.D. journey. Especially to my supervisor and her team.

Finally, I am indebted to my Ph.D. journey in UTeM, Ummu, Djah, Siti, Ayu, Kanaga, Filda, Kak Su, Mas and many other Ph.D. students. Thank you for providing me emotional and spiritual support that I have enough confidence to face the challenges during the thesis preparation. I am so grateful to have them share my pieces in my life.

TABLE OF CONTENTS

PAGE

DECLARATION
APPROVAL
DEDICATION
ABSTRACT **i**
ABSTRAK **ii**
ACKNOWLEDGEMENTS **iii**
TABLE OF CONTENTS **iv**
LIST OF TABLES **viii**
LIST OF FIGURES **x**
LIST OF APPENDICES **xii**

CHAPTER
1. INTRODUCTION **1**
1.1 Background 1
1.2 Insider threats 9
1.3 Challenges on insider threats problems 12
1.4 Problem statement 15
1.5 Research questions 20
1.6 Research objectives 21
1.7 Scope of research 23
1.8 Significance of research and contributions 25
1.9 Operational definition of key terms 28
1.9.1 Cyber security 28
1.9.2 Vulnerability 28
1.9.3 Insider threat 29
1.9.4 Personality characteristics 29
1.9.5 Psychological State 30
1.9.6 Motivation to attack 30
1.9.7 Skill-set captures 31
1.9.8 Opportunity 31
1.9.9 Historical behaviour 32
1.9.10 Precipitating event 32
1.9.11 Organisational performance 33
1.10 Structure of thesis 33
1.11 Summary 34

2. LITERATURE REVIEW **36**
2.1 Introduction 36
2.2 Insider threats' search result 37
2.3 Insider threats' definitions and statements 39

2.4 The factors governing cyber security and its relationship 45
2.5 Organisational performance 51
2.5.1 Environmental performance 53
2.5.2 Economic performance 54
2.5.3 Social life performance 54
2.6 Sample of insider threats' real cases 55
2.7 Theoretical reviews of insider threat characteristics 60
2.8 Conceptual framework of insider threat characteristics 67
2.9 Summary 79

3. RESEARCH METHODOLOGY 80
3.1 Introduction 80
3.2 Research paradigm 80
3.3 Research philosophy 81
3.3.1 Approaches 85
3.3.2 Strategies 87
3.3.3 Choice 87
3.3.4 Time horizons 88
3.3.5 Techniques and procedures 89
3.3.6 Research design 90
3.4 Target respondents and sampling 93
3.5 Unit of analysis 97
3.6 Research framework 100
3.7 Theoretical basis of using Structural Equation Modelling (SEM) 104
3.7.1 Comparing Covariance Based-SEM (CB-SEM) and Partial Least Square-SEM (PLS-SEM) 104
3.8 Operationalisation of variables 105
3.8.1 Development of measures for variable construct 108
3.9 Research instrument – questionnaire 111
3.9.1 Pre-testing and pilot testing of questionnaire 112
3.9.2 Final questionnaire 114
3.10 Population and sampling 116
3.10.1 Sample size 118
3.10.2 Key informant 119
3.10.3 Data collection process 120
3.11 Data analysis procedures 121
3.11.1 Structural Equation Modelling (SEM) 121
3.12 Summary 124

4. DISSCUSSION ON METHOD OF THE STUDY 125
4.1 Introduction 125
4.2 Definition triangulation 125

4.2.1 Types of triangulation method 126
4.2.2 Triangulation method 127
4.3 Semi structured interview 129
4.4 Small group discussion with panel (expertise) 131
4.4.1 Participant demographics 133
4.4.2 Interview protocol and process 135
4.4.3 Emerging themes 136
4.5 Conclusion 143
4.6 Summary 145

5. RESULT AND DISCUSSION 146
5.1 Introduction 146
5.2 Sample size 147
5.3 Sample characteristics 147
5.3.1 Background of respondents 149
5.3.2 Education, position, and years of employment 150
5.3.3 Functional and region 151
5.4 The Confirmatory Factor Analysis (CFA) 158
5.5 Validating the latent construct using Confirmatory Factor Analysis (CFA) 159
5.5.1 The Confirmatory Factor Analysis (CFA) 159
5.6 The measurement model for actor characteristic construct 161
5.7 The CFA procedure for validating actor characteristics construct 162
5.8 The assessment for construct validity 162
5.9 The assessment for convergent validity and composite reliability 163
5.10 The measurement model for organisational performance construct 165
5.11 The CFA procedure for validating organisational performance construct 166
5.12 The assessment for construct validity 167
5.13 The assessment for convergent validity and composite reliability 169
5.14 The pooled-CFA for all measurement model of constructs 171
5.15 The assessment for convergent validity and composite reliability 173
5.15.1 Validating the measurement model for all components of actor characteristics 179
5.16 The assessment for construct validity 179
5.16.1 The assessment for convergent validity and composite reliability 179
5.17 The assessment of normality for items of all constructs 181
5.18 The structural model and Structural Equation Modeling (SEM) 186
5.19 The structural model for testing the components of actor characteristics 186
5.20 Discussion of the findings 191
5.21 Summary 194

6. CONCLUSION AND RECOMMENDATIONS 196
6.1 Introduction 196
6.2 Summary of the study 199
6.3 Discussion of results (table of summary-objective) 204
6.4 Contribution 204
6.4.1 Theoretical contribution 204
6.4.2 Contribution and implication industry 207
6.4.3 Contribution and implication for government 210
6.4.4 Contribution and implication for Malaysian organisation – profiling (screening) mobile apps design 213
6.4.4.1 Mobile apps design 215
6.5 Limitations of the study 218
6.6 Recommendation and future research directions 220
6.6.1 Lack of employee screening – justification of mobile apps design 224
6.6.2 Employee screenings – justification of mobile apps design 225
6.6.3 Human behaviour 226
6.6.4 Understanding pressure, opportunity and rationalisation from the fraud triangle 227
6.6.5 Lack of awareness 229

REFERENCES 231
APPENDICES 269

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Research problem (RP) statements	20
1.2	Research questions	21
1.3	Research objectives	21
2.1	CMU – CERT’s insider threat definition	40
2.2	FBI’s insider threat definition	41
2.3	Shaw, Fisher and Rose’s insider threat definition	41
2.4	Matt Bishop’s insider threat definition	41
2.5	Brackney and Anderson’s insider threat definition	42
2.6	Elements	50
2.7	Sample case study	57
2.8	Insider threats characteristics based on CMU_CERT, APA, SBT theory	73
3.1	Comparison of four research philosophies in management research (Saunders et al., 2012)	83
3.2	Summary of research design elements	98
3.3	Operationalisation of variables utilised in this study	106
3.4	Development of measures for the potential characteristics of the insider threat elements	108
3.5	Development of measures for precipitating event elements	109
3.6	Development of measures for performance of industrial manufacturing	110
3.7	Growth of Malaysia’s manufacturing sales by sector (DOSM, 2019)	117
5.1	Demographic data of the respondents	147
5.2	Education, position and years of employment data of the respondents	149
5.3	Functional area and region data of the respondents	151
5.4	The three categories of model fit and their level of acceptance	153
5.5	The main hypothesis of interest and method of analysis	155
5.6	The hypothesis of interest for every component of actor characteristic	157

5.7 The Average Variance Extracted (AVE) and Composite Reliability (CR) 164
5.8 The Average Variance Extracted (AVE) and Composite Reliability (CR) 168
5.9 The Average Variance Extracted (AVE) and Composite Reliability (CR) 171
5.10 The Average Variance Extracted (AVE) and Composite Reliability (CR) 176
5.11 The discriminant validity index summary for all constructs 178
5.12 The assessment of normality for all items and components 179
5.13 The coefficient of multiple determination or R^2 and its implication in this study 183
5.14 The regression path coefficient between construct and its significance 184
5.15 The hypothesis testing for direct effect hypothesis 185
5.16 The hypothesis for testing mediation effect of participating event 185
5.17 The effect of every component of actor characteristic on precipitating event 189
5.18 The regression path coefficient between construct and its significance 190
5.19 The hypothesis testing for direct effect hypothesis 190
6.1 Summary of research questions and key findings 199

LIST OF FIGURES

FIGURE	TITLE	PAGE
1.1	Cybercrime statistics (2018 and 2019)	38
2.1	Factors affecting organisational behaviour (Richards, 2017)	47
2.2	Factors governing cyber security and the relationship between technology, organisation, and human (Muniandy and Muniandy, 2012)	49
2.3	Sample of cyber-attack in the news from November 2017 to March 2021 in Malaysia	56
2.4	Theoretical reviews, framework for characterising insider threat (Nurse, et al., 2014b)	60
2.5	Conceptual Framework - Framework for Characterising Insider Threat (Costa, 2017, Nurse et al., 2014b)	67
3.1	Research framework	103
5.1	The research framework of the study and hypothesis of interest	154
5.2	The research framework testing the components of actor characteristic	156
5.3	The measurement model for actor characteristics construct	161
5.4	The CFA results for actor characteristics construct	162
5.5	The measurement model for organisational performance	165
5.6	The CFA results for organisational performance construct	167
5.7	The CFA results for the pooled-measurement model of three constructs	170
5.8	The CFA for all components of actor characteristics	173
5.9	The CFA results for all components of actor characteristics	174
5.10	The structural model for the main hypothesis of actor achievement	182
5.11	The standardised regression path coefficient between contracts	183
5.12	The results for regression path coefficient between constructs	184
5.13	The procedures for testing the mediator precipitating event	186
5.14	The second structural model of the study in IBM SPSS AMOS	187
5.15	The standardised regression weight between the constructs	188
5.16	The regression path coefficient estimates for the model	189

6.1 Splash screen 215
6.2 Home screen 216
6.3 Question section A 216
6.4 Question section B, C and D 217
6.5 Result screen 217
6.6 Google spreadsheet as database to store data 218

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Invitation letter	269
B	Research instrument	271
C	Assessment of normality	277
D	The hypothesis testing for direct effect hypothesis	278
E	Publication	279
F	Turnitin	280

CHAPTER 1

INTRODUCTION

1.1 Background

According to a recent Ponemon Institute, 2019 report 60% of all data breaches are caused by insider threats. This emphasizes how crucial it is to have strong cybersecurity procedures in place to protect the company from internal risks as well as external adversaries.

One notable case is that of the Equifax data breach in 2017, which was traced to an employee who failed to patch a known vulnerability in the company's system despite multiple warnings from the company's IT department. This resulted in the personal data of over 147 million Americans being compromised.

Another example is the Capital One data breach in 2019, which was caused by a former employee who exploited a misconfigured firewall to gain access to sensitive customer data. The breach affected over 100 million customers and led to the arrest of the perpetrator.

There have also been instances where employees unintentionally caused cyber incidents through actions such as clicking on a malicious link or falling victim to a phishing scam. In a study by IBM, it was found that human error accounted for 95% of cybersecurity incidents and breaches.

To mitigate the risks posed by insider threats, organisations need to adopt a multi-layered approach that includes regular training and awareness programs for employees, strong access controls and monitoring processes, and robust incident response plans.

Additionally, organisations should conduct regular assessments to identify areas of vulnerability and implement appropriate measures to address them.

In conclusion, insider threats continue to pose a major challenge to organisations when it comes to cybersecurity. It is essential for organisations to not only focus on external threats but also to be proactive in managing risks from inside the company indirectly can risk the organisational performance.

One of the most notable cases of insider threat in Malaysia was the cyber-attack on the government-linked company, Malaysian Airlines in 2015. The attack was carried out by a former employee who had access to the company's systems and was able to steal confidential data, including passenger information and flight records. The incident had a significant impact on the organisation's performance, as it compromised the trust and confidence of customers and stakeholders. It also led to financial losses for the airline as it had to compensate affected customers and invest in cybersecurity measures to prevent future attacks.

Another case of insider threat in Malaysia was the theft of trade secrets by an employee of a multinational technology company in 2018. The employee, who was responsible for product development, stole confidential information and shared it with a competitor. This led to a loss of competitive advantage for the company and negatively impacted its financial performance.

There have also been cases of employee misconduct in the banking and financial sector in Malaysia. In 2017, a bank employee was charged with embezzling over RM10 million from a client's account, which negatively impacted the bank's reputation and credibility. In another case, an employee of a financial institution was involved in a fraudulent scheme that caused losses of millions of ringgits to the institution and its clients.

This research work is to study exploring threats using organizational performance framework in Malaysian manufacturing case. McKinsey and Company states that many organizations are struggling to define the insider threats which arise from their employees who are negligent and those with malicious intent. According to Verizon's 2021 Data Breach Investigations Report, contractors are typically considered insiders in the context of cybersecurity. An insider threat refers to the risk posed by individuals within an organization, and this category includes not only regular employees but also contractors, consultants, or any third-party personnel who have access to the organization's systems, networks, or sensitive information. Contractors often have specific roles or projects within an organisation that require them to access internal systems and data. While they may not be permanent employees, their access to sensitive information makes them potential insider threats if proper security measures are not in place. The risk associated with contractors, both unintentional (negligent) and intentional (malicious), is taken into consideration when organizations develop strategies to manage insider threats.

Although they are thought to be challenging to forecast and avoid, insider threats pose a severe hazard to organisations. Despite the fact that a growing body of research has looked at personological precursors to insider threats, there is no overarching theoretical framework that connects the investigated traits in this literature. This review lists the personality traits that have been linked to insider threat behaviors and suggests neo-psychoanalytic theory as a useful framework for classifying these traits and separating insider threats from accidents in the workplace and counterproductive work behaviors. (Marbut and Harms, 2023).

Overall, insider threats in Malaysia have had a significant impact on organisational performance and highlighted the importance of effective security measures and employee training to prevent such incidents from occurring. One research article that discusses the impact of insider threat on organizational performance in the industrial manufacturing industry is "Insider threat: A systematic review of the literature and research agenda for future studies" by Liu et al. (2017). The article highlights the potential consequences of insider threats, such as financial loss, damage to reputation, and loss of intellectual property, which can all directly impact organizational performance.

One example is the case of a former engineer at a semiconductor company in Malaysia who was sentenced to 10 years in prison for stealing trade secrets and technology from his former employer and attempting to sell them to a Chinese company (Robertson and Riley, 2022).

There is another example of cases from manufacturing of Malaysian company, all the cases were reported from Daily express media and Star Online media headlines over the years.

i. In 2013, an employee at a Malaysian manufacturing company was arrested for allegedly stealing nearly RM 3 million (around USD 715,000) worth of cables and selling them to a scrap metal dealer.

ii. In 2015, a production manager at a Malaysian steel company was charged with stealing raw materials worth over RM 1 million (around USD 238,000).

iii. In 2018, an employee at a Malaysian car parts manufacturing company was caught stealing spare parts worth RM 50,000 (around USD 12,000) and was sentenced to five years in prison.

iv. In 2020, a former employee of a Malaysian metal manufacturing company was arrested and charged with stealing copper wire worth RM 150,000 (around USD 35,000).

v. In 2017, an insider threat caused Xingfa Aluminium Holdings Bhd, a Malaysian firm, to disclose a RM1.6 million loss. The business learned that one of its workers had been defrauding consumers of their money by sending false invoices.

vi. In 2019, a logistics company called GDEX Berhad reported that one of its employees had stolen a parcel containing high-value items worth RM140,000. The employee was identified and arrested, and the stolen items were recovered.

vii. In 2020, Inari Amertron Berhad, a Malaysian semiconductor manufacturer, that a staff member had pilfered a shipment of microchips valued at roughly RM1.5 million. The worker was located, fired, and then taken into custody.

These cases show that insider threats can have a significant impact on industrial manufacturing companies in Malaysia, including financial losses and damage to reputation. It highlights the importance of implementing strong access controls and monitoring systems to detect and prevent these types of incidents.

Traditional notions of cyber security place an emphasis on protecting against attacks that arise from external threats. However, it is becoming increasingly apparent that the greater threat to an organisation’s security may well lie within, as evidenced in many recent surveys. There are several classes of elements, depicted in four areas, namely Attack catalyst, Actor characteristics (i.e., those of a potential insider threat), Attack characteristics, and Organisation characteristics. For this study, the researcher triggered that there was big impact on the organisational performance and these issues will become normalising if the insider threat still running in the organisation. Therefore, the researcher wants to explore the insider threat characteristics or attack characteristics focus more on the human behaviour and social science context using organisational performance framework in manufacturing case. Even out there have a lot of ways with advance technology, system, process in the cyber security area in order to protect the confindential data, property, information of the company, however the first thing first that need to be identified and understanding is the human trust or the human itself. Human is the person who have the authorised power, knowledge, idea. Human also is the person who have the emotional parts in their life and sometimes it will become hidden agenda in silent mode. Abdullah, Saufi and Nor, (2021).

For this study, six elements are identified in modelling and analysing the aspect of insider threats. The elements are: i) Precipitating Event (as mediator), ii) Individual's Personality Characteristics, iii) Historical Behaviour, iv) Psychological State, iv) Motivation to Attack, and v) Skill Set and Opportunity. An empirical study will be conducted to further construct the components that constitute insider threats. A theoretical model will be developed using a baseline model that states the factors associated with an insider attack, which are psychological, behavioural, and motivation and intention. Second generation statistics will be used as an analytical tool to measure the relationship between construct factors. The contribution of this study can be divided into two major parts, which are theoretical contribution that consists of potential factors associated with predicting an insider attack. In this case, characteristics of an insider attack will further be developed and improved.

The threats that insiders pose to organisations continue to be of serious concern and are not something new and unusual to most companies in Malaysia. Recent industry surveys and academic literature provide clear evidence to support the significance of these threats. However, most of these companies choose not to confront the risk openly and prefer to handle it in a subtle way. Companies are reluctant to state their experience and difficulties dealing with issues related to insider threats. This is probably due to adverse reputation and fear that revealing the fact that trusted people within the organisation commit wrongdoing or fraud will further have an undesirable impact on the company's operations and customers' perception. Such incidents of insider attacks could result in reputation loss for the affected organisation (Ford and Backhoff, 2019).

However, many organisations are denying that the problem of insider threats even exists. There is still no framework to fully characterise insider threats and to facilitate and understand their impact on organisational performance. Therefore, this research will look into the insider threat characteristics and their impact on organisational performance through a grounded framework to understand and reflect on the threats that insiders pose.

The framework will identify several key characteristics of insider threats within the selected organisation, focusing on the manufacturing industry in Malaysia, concentrating on indicators that consist of actor and organisation characteristics and type of attack. The real value of the framework is in its emphasis on bringing together and clearly defining the various characteristics of an insider threat. This framework is based on real-world cases and pertinent literature and has an impact on organisational performance. This can therefore act as a platform for general understanding of the threat and also for reflection on related organisations.

This research work aims to exploring insider threats characteristics by using organisational performance framework in Malaysian manufacturing case. Insider threat emerged and were chosen for this study's focus due to the need to fully research and comprehend them from the standpoint of this nation. It is crucial, especially given that the Malaysian government has acknowledged that insider threats pose a serious risk to the company (Malaysia Cyber Security Strategy, 2020). Nevertheless, there are still not enough research from the standpoint of Malaysia despite the government's acknowledgement. This was made clear by a document or journal submission search result in the Elsevier Scopus® online portal (last evaluated on March 31, 2022).

According to IBM Security's report from 2021, 40% of incidents were discovered as a result of alerts produced by internal monitoring software, 100% of incidents involved situations in which insiders had administrative access, and 40% of incidents involved an employee with privileged access to company property. 10,016 incidents were totaled for the year 2021, with spam accounting for 102 (1.02%), intrusion accounting for 1410 (14.08%), vulnerabilities reported for 69 (0.69%), intrusion attempts for 159 (1.59%), denial of service for 22 (0.22%), malicious code accounting for 648 (6.47%), and content-related incidents accounting for 91 (0.91%). Bailey et al. (2018) states that many organisations are struggling to define (identify) insider threats that arise from their employees who are negligent or those with malicious intent. In this case, contractors are also considered employees or insiders.

There are many literature reviews from books, articles, journals, etc., narrating insider threats, which are made available for our reference. Observation from the online portal keyword of SCOPUS and GOOGLE SCHOLAR, every year the cases is increasing incrementally and from paper itself considering these cases has become a critical case in the world and it need get the best solution in order to mitigate these issues of insider threat.
This situation was evidently indicated from online search via the SCOPUS portal on October 10, 2023. The word "*insider threat*" was entered as the keyword in the SCOPUS online portal. Based on the keyword, it produced 11,776 results on related insider threat document submissions from 52 different countries. Within the last five years, only 7821 papers from various countries have been published, 606 with papers from Malaysia ranging from computer science, business accounting, economic, and social sciences area and 217 result on related paper from social science from 2000 until 2023. Clearly indicated from online search via the GOOGLE SCHOLAR portal on October 10, 2023. The word "*insider threat*" was entered as the keyword in the GOOGLE SCHOLAR online portal. Based on the