INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 3, (2025) E-ISSN: 2222-6990

Discovering the Impact: Exploring How Insider Threat Drivers Relate to Organizational Performance

Sedek M[1], Omar S.R[2], Isnin S.N[3]

[1,2]Centre for Language Learning, Universiti Teknikal Malaysia Melaka, 76100 Durian Tunggal, Melaka, Malaysia, [3]Faculty of Technology Management andTechnopreneurship, Universiti Teknikal Malaysia Melaka, 76100 Durian Tunggal, Melaka, Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v15-i3/24976 DOI:10.6007/IJARBSS/v15-i3/24976

Published Date: 10 March 2025

Abstract

This study aims to investigate the determinants of Insider Threat Drivers and the impact on organizational performance. By understanding these determinants, organizations can generate awareness to protect themselves and mitigate potential insider threats by recognizing their characteristics. The findings reveal a significant relationship between individual personality traits, motivation to attack, psychological state, skill set, opportunity, and individual characteristics with the propensity for insider threats and concern for precipitating events. Additionally, the study shows a significant relationship between insider threat drivers and organizational performance. This research is crucial as it provides guidelines, instructions, andawareness to support organizations, employers, and researchers in mitigating potential insiderthreats. By understanding the underlying factors that contribute to insider threats, organizationscan implement targeted strategies to enhance security and protect their assets.

Keywords: Exploring, Insider Threat Drivers, Organizational Performance, Significant Relationship

Introduction

Data breaches, insider threats, and cyber-attacks are not new phenomena. Federal agencies have long acknowledged the ongoing hazard of exploits. However, 2019 saw unprecedented attacks, even on previously considered unbreachable systems. Almost nine months into 2019, it had already been a banner year for cybersecurity incidents, affecting both government entitiesand private businesses. A slew of insider threats, including data breaches, malware, and backdoor attacks, exposed hundreds of millions of users' private data in 2019. According to Aaron Holmes from Business Insider US, most high-profile hacks in 2019 appeared to be financially motivated, although some were traced back to governments aiming to monitor individuals (Holmes, 2019). Insiders often have various motives for becoming attackers, such as financial gain, corruption, and revenge.

In 2018, cybersecurity threats were projected to cost organizations in Malaysia US$12.1 billion in economic losses (Paramasivam, 2018). A study by Microsoft and Frost & Sullivan revealed that a large organization in Malaysia might incur an economic loss of US$22.8 million due to cybersecurity incidents, more than 630 times the average economic loss for a mid-sized company. Additionally, malware threats resulted in job losses in 61% of companies over the last three to five years. These incidents significantly impact organizational performance, particularly economically (Sedek, & Mohd, 2025).

Although threats can manifest through technology, systems, processes, and human actions, thehuman element remains one of the most critical aspects of protection. People tend to trust those they know, leading them to share passwords or other sensitive information inappropriately. Insider threat actions are almost always preceded by a deliberate decision, resulting in either intentional or accidental consequences. Understanding human behavior and decision-making is vital to protecting against insider threats. Defense against such threats requires an active focus on workplace behavior (Cline, 2016; Colwill, 2010). A better understanding of human characteristics helps explain why insider threats behave in certain ways and how to identify and mitigate potential insider threats.

Therefore, this study aims to investigate the determinants of Insider Threat Drivers and their impact on organizational performance. By understanding the characteristics of potential insiderthreats and the factors that drive these threats, organizations can generate awareness and implement measures to protect themselves. Profiling and screening the characteristics of employees can aid in mitigating potential insider threats effectively.

Understanding Insider Threat

There is extensive and ongoing research on insider threats, resulting in security solutions released to the market. However, these solutions are not as readily accepted as those for external threats (Hong et al., 2010). Insider threat definitions vary across different studies, encompassing individuals such as employees, contractors, or service technicians who may inadvertently have insider access. A malicious insider specifically refers to someone motivated to intentionally harm an organization's mission by adversely impacting its operations through actions like denial, damage, degradation, or destruction of assets.

An insider, with respect to security rules, is a user trusted to take certain actions according to established guidelines but poses a risk if they violate those rules. Insider risk encompasses thepotential for trusted or authorized individuals to engage in behaviors that harm their employer,posing significant threats to national and corporate security. The most concerning threat oftencomes from insiders with legitimate access, as they may exploit their privileges for personal gain or on behalf of external entities, such as competitors or foreign nations.

Insider risk poses a considerable challenge to organizations. Trusted individuals with authorized access can abuse their privileges, compromising the confidentiality, integrity, or availability of information or systems. This underscores the importance of implementing robust security measures, monitoring systems, and insider threat detection programs to mitigate these risks effectively. According to the CA Insider Threat Report, 90% of organizations feel vulnerable to insider attacks. Key risk factors include excessive access

privileges for too manyusers, an increasing number of devices with access to sensitive data, and the growing complexity of the IT environment. The CA survey revealed that 53% of respondents confirmedinsider attacks against their organization in the past 12 months, with 27% noting an increase infrequency. Organizations are focusing on detecting insider threats (64%), deterrence methods (58%), and post-breach forensics (49%).

User behaviour monitoring is on the rise, with 94% of organizations deploying methods to monitor users and 93% tracking access to sensitive data. Prevalent technologies to deter insider threats include Data Loss Prevention, encryption, and Identity and Access Managementsolutions. To detect active insider threats, companies use Intrusion Detection and Prevention Systems (IDS) and Security Information and Event Management (SIEM) platforms. A vast majority (86%) of organizations have built their own insider threat programs, with 36% havinga formal program in place and 50% focused on developing one (Schulze, 2018).

Insider threats constitute a significant cybersecurity challenge, arising from various categoriesof individuals with access to organizational assets. Employees, integral members of theorganization, have significant access to resources and data. According to Verizon's 2020 report,30% of security events, including data breaches and asset misuse, were attributed to insider threats from employees. This highlights the critical importance of addressing internal vulnerabilities.

Partners, including suppliers, vendors, contractors, and consultants, also pose potential insiderthreats. Despite their collaborative roles, they may inadvertently or intentionally risk the organization's security. The same Verizon report noted that insider risks from partners accounted for 14% of security incidents, emphasizing the need for close management of accessand privileges for external collaborators.

Contractors, engaged on a project-by-project or temporary basis, introduce additional complexities to insider threat mitigation. While they may possess specialized knowledge beneficial to the organization, they also present potential security risks. The 2018 Ponemon Institute poll found that insider threats from contractors contributed to 16% of security incidents, underlining the importance of monitoring and managing their access to sensitive assets.

In summary, insider threats can originate from a diverse array of sources within an organization, including employees, external partners, and contractors. The likelihood of insiderthreats is influenced by factors such as the nature of work and the level of access granted. To effectively mitigate these risks, organizations must implement robust security measures, continuous monitoring, access controls, and employee awareness training to protect sensitive information and assets from unauthorized access or misuse.

Insider Threat Drivers

Based on previous research that collected case data, the researcher identifies eight elements crucial for modeling and analyzing insider threats. These elements are the Precipitating Event or catalyst, the individual’s Personality Characteristics, Historical Behaviour, Psychological State, Skill Set and Opportunity, and Motivation to Attack (Nurse et al., 2014, Costa, 2017).

For this study, these elements have been consolidated into five key components, which will bediscussed in further detail.

The study adopts these elements and introduces a new model of Insider Threat Drivers (ITD), incorporating actor characteristics (AC) and the precipitating event (PE) as a mediator. Additionally, this study includes organizational performance as a new variable. Below is a comprehensive summary of the key components and their integration into the new ITD model:

Actor Characteristics (AC)

Personality Characteristics: These encompass the inherent traits and behaviors unique to individuals, which may incline them towards engaging in insider threats. Factors such as impulsivity, lack of empathy, or susceptibility to coercion can contribute to the manifestation of insider threat behavior.

Historical Behaviour: Examining past actions and behaviors provides valuable insights into an individual's propensity for insider threats. Patterns of misconduct, previous security breaches, or disregard for organizational policies serve as red flags that warrant closer scrutiny.

Psychological State: The mental and emotional well-being of individuals significantly influences their decision-making and behavior. Psychological factors such as stress, discontentment, or feelings of disenfranchisement can exacerbate the likelihood of insider threat incidents.

Skill Set and Opportunity: The combination of an individual's capabilities and the availabilityof opportunities plays a pivotal role in facilitating insider threat activities. Individuals with specialized skills or privileged access to sensitive information are more likely to exploit vulnerabilities within the organization.

Motivation to Attack: Understanding the underlying motivations driving insider threat behavior is crucial for effective mitigation strategies. Motivations may vary widely, ranging from financial gain and personal grievances to ideological beliefs or coercion by external entities.

Precipitating Event (PE): A precipitating event serves as a triggering factor that catalyzes insider threat behavior. These events could include personal crises, workplace conflicts, or significant changes in organizational dynamics, prompting individuals to act on their motivations and exploit their characteristics.

Organizational Performance

Organizational performance is a key aspect of an organization's ability to achieve its objectives and maximize outcomes in today's dynamic business environment. While performance measures help organizations track their progress, various factors such as market conditions, firm size, and internal resources influence performance. Performance measurement has become a popular research topic, with frameworks and measures developed to aid

organizations in evaluating their goals and objectives. (Neely et al., 2002; Ford & Backhoff, 2019; Madeline Miles, 2022)

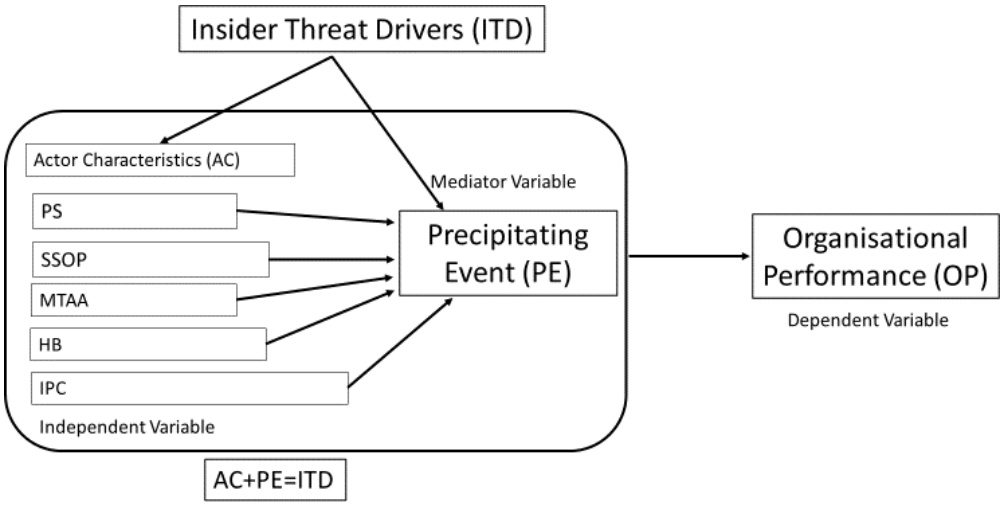
In the context of insider threats, monitoring organizational performance can aid in detecting suspicious behavior early on. By utilizing performance data, organizations can implement targeted security measures and training to effectively mitigate insider threats. Recent research highlights the importance of considering organizational performance metrics in addressing insider threats, emphasizing dimensions such as environmental, social, and economic performance.

To mitigate insider threats and enhance organizational performance, it is essential to focus on three primary areas: environmental performance, social life performance, and economic performance. By addressing the multifaceted nature of insider threats and fostering a culture ofcontinuous improvement and vigilance, organizations can bolster their resilience to internal risks and safeguard their sensitive information and assets.

Understanding the potential characteristics of insider threats and adopting proactive cybersecurity measures are crucial steps for organizations to safeguard their performance and protect against internal threats.

Organizational Performance: Insider threats can have profound ramifications on organizational performance, encompassing financial losses, operational disruptions, damage toreputation, and erosion of stakeholder trust. Assessing the impact of insider threats on various facets of organizational performance is essential for devising effective risk management strategies.

In summary, this study refines previous qualitative method into a triangulation method, introducing a new model of Insider Threat Drivers (ITD) that integrates actor characteristics, precipitating events, and organizational performance. This approach enhances the ability to predict, detect, and mitigate insider threats, ultimately safeguarding organizational assets and integrity.



Figures 1: Insider Threat Drivers (ITD) Framework

Actor Characteristics

The Precipitating Event, serving as a mediator in this paper, is the key event or catalyst that has the potential to push an insider over the edge, transforming them into a threat to their employer. This concept, initially referred to as the 'tipping point' in insider-threat literature, encompasses events such as employee dismissal, disputes over intellectual property rights, perceived injustices, negative company actions like layoffs, family problems (e.g., divorce, child custody issues, health problems), coercion, new job opportunities offered by competing companies, or even lack of training leading to accidental attacks. Research in counterproductive workplace behavior has been crucial in defining and understanding these events, as well as their connection to human behavior and workplace aggression.

Individual Personality Characteristics include psychological traits and dispositions that reflect an actor's personality, based on both their innate self (static aspects) and their life experiences(dynamic aspects). General personality traits can be described using the OCEAN model (Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism). Other relevant characteristics might include maturity, aggressiveness, social skills problems, superficiality, (lack of) self-esteem, and personal integrity.

Historical Behaviour documents the types of activities an actor has engaged in over time, which are often influenced by their personality characteristics. Examples of notable behaviors from amalicious insider-threat perspective include addictive practices such as gambling or alcohol abuse. In the case of unintentional threats, relevant behaviors are typically the result of humanerror, such as carelessness or absent-mindedness.

Psychological State represents the actor's current psychological and emotional condition (e.g.,happiness, depression, stress, or anxiety). This state may stem from their psychological makeup(e.g., clinical depression) or environmental factors (e.g., a stressful event like a forced job transfer leading to depression). This explains the relationships between psychological state, personality characteristics, and precipitating events (Clark & Watson, 1988; Martinko, Gundlach, & Douglas, 2002; Liang & Biros, 2016).

Motivation to Attack captures the reasons an actor might want to harm the company. The concept of attack motivation is well understood in threat assessment, and this study draws heavily on existing work to define general categories of motivation (Martinko, Gundlach, & Douglas, 2002; Nurse, Buckley, Legg et al., 2014).

Skill Set encompasses the abilities or skills an actor needs to conduct an attack. There is often a link between the actor's role within an organization and their skill set, although individuals may possess skills beyond their job role (Jones & Ashenden, 2005).

Opportunity represents the chance for the actor to launch an attack on the company. The concept of opportunity to attack is well defined in the literature on threat assessment and risk management (Nurse, Buckley, Legg et al., 2014; Sohrabi, Maple, Watson, & Solms, 2017).

In summary, this study integrates these elements into a comprehensive framework for understanding and mitigating insider threats. By examining the interplay between actor

characteristics, precipitating events, and organizational performance, the research provides valuable insights for enhancing security measures and reducing the risk of insider threats.

Methodology

This research aims to provide a comprehensive framework model detailing insider threat drivers (characteristics and factors) and their impact on organizational performance. A literature review revealed that all the characteristics mentioned in this study play crucial roles in the formation of insider threats. The research model is built on five key elements and a mediator variable (precipitating event), extending from previous studies.

To validate the research model, experts in the domain were consulted to review the model, validate the questionnaires, and provide their opinions on whether the conceptual model aligns with their experience and knowledge. Their endorsement confirmed the model's relevance. Theframework's development leveraged both quantitative methods and focus group interviews with experts, employing a triangulation approach to enhance methodological rigor. A questionnaire employing a five-point Likert scale was developed based on the main factors andinsights from previous studies. To expedite data collection, both electronic and paper-based questionnaires were used.

The research model was developed based on four foundational theories, i) CMU-CERT (Carnegie Mellon University, Computer Emergency Response Team), ii) APA (American Psychiatric Association), iii) SBT (Social Bond Theory) and iv) TPB (Theory of Planned Behaviour), particularly focusing on the precipitating event orbehavior intention.

A thorough literature review also informed the model's development. Confirmatory Factor Analysis (CFA) was considered appropriate for validating the model, and Structural Equation Modelling (SEM) was used to test its reliability and validity. Triangulation methods were employed to ensure robustness and comprehensive validation of the framework. This approach combined multiple data sources and methods, including quantitative analysis, expert interviews, and theoretical foundations, to enhance the reliabilityand depth of the research findings.

In summary, this research introduces a validated framework model that integrates insider threatcharacteristics, precipitating events, and their impacts on organizational performance. The useof triangulation methods, expert validation, and robust statistical analysis ensures the model's applicability and effectiveness in understanding and mitigating insider threats.

Sample Selection and Data Collection

Data was collected from staff across several manufacturing industries in Malaysia, including those involved in operations, production, information technology, and human resources. The goal was to educate and raise awareness among employees who may overlook the threat and to reinforce the importance of information security for those already familiar with it. Data gathering took place from July 2019 to the end of December 2019.

The questionnaire was developed based on a thorough understanding of the factors outlined earlier and incorporated insights from previous studies in this field. Responses were

measuredusing a five-point Likert scale, ranging from "strongly disagree" to "strongly agree." All instruments were validated by an expert panel to ensure their relevance and accuracy.

Population of this study comes from manufacturing firms that are registered Department of Statistics Malaysia, Malaysia's Industrial Production Index 2018. (DOSM, 2018). Sample has been randomly selected among seven types of manufacturing industries under transport equipment and others manufacturers known as automotive industry, materials industry, auto parts industry, transportation equipment industry, technology equipment industry, telecommunication equipment industry and health care equipment industry by using stratified random sampling technique. The key respondents for this study were CEOs, managers, executives and supervisors from manufacturing industry that have extensive experience and knowledge on awareness of insider threat. This study utilized both mail and online survey questionnaire for data collection. Out of 500 distributed questionnaire, data collection from both methods gathered 352 returned were found usable for this study.

Table 1
Questionnaires of mediator, potential insider threat characteristics and organisational performance

Statement/Penyataan	***Mean***	***Sd***
THE PRECIPITATING EVENT (Mediator) *MEMPERCEPATKAN PERISTIWA*		
I have no intention to accept any offer (gift/part-time job) from others organisation at the moment.	4.08	0.64
I have never shared confidential issues of the organisation to the outsider.	4.29	0.75
I never been offered a gift by the outsider that want me to share the information of the organisation.	4.17	0.74
I am interested to attend training programme about security in my organisation.	4.27	0.78
INDIVIDUAL PERSONALITY CHARACTERISTICS *PERSONALITI KRITERIA SESEORANG*		
I respect my organisational procedures and policies.	3.31	0.99
Organisational information and security plan are most important for me.	3.06	0.89
I have an intention to avoid any misbehaviour.	3.75	0.95
I obey information security policies in my organisation to avoid misbehaviour	3.75	0.91
I am actively participated, like to in-charge and organise the organisation activities	3.73	0.82
HISTORICAL BEHAVIOUR *SEJARAH TINGKAH LAKU*		
I do not always feel pressured at the workplace.	2.81	0.60
I will not do an unethical behaviour if I feel depress.	3.16	0.96
I will not share confidential information of the company to the outsiders.	2.43	0.65
I will act professionally towards a person who made mistakes with me in theorganisation.	3.22	0.88
PSYCHOLOGICAL STATE *KEADAAN PSIKOLOGI*		
I feel the excitement with no stress working in this organisation.MTA	3.18	0.60
I always feel appreciate in this organisation.	3.75	0.75

I believe my employers always look after workers' welfare.	3.69	0.85
I have the awareness of the important of trust in the organisation.	4.05	0.50
MOTIVATIONAL TO ATTACK *MOTIVASI UNTUK ANCAMAN*		
I am a very professional person.	3.84	0.66
I am not a person who like to revenge to the others.	3.84	0.66
I am a good worker and obey with rules and regulation in the organisation.	3.82	0.66
I am committed to follow organisation rules and regulation.	3.82	0.66
SKILL-SET AND OPPORTUNITY *MENUJUKKAN KEMAHIRAN DAN PELUANG*		
I always work hard to get information related to a new software.	4.06	0.67
I like new application and software.	4.03	0.74
I have the desire to be excellent skill in software development.	3.75	0.83
I am programmer	3.65	0.79
I have the ability to work for people who give me a better payment.	3.84	0.63
I do not bother if anyone gives me a gift and asks for information about thecompany.	3.84	0.63
I will try to defend myself from accepting a fair offer.	3.83	0.64
Environment **I perceived that my organisation has: -**		
a better workplace quality.	4.12	0.91
an improve welfare quality for the employees.	3.91	0.91
an improve of good air quality and noise pollution.	3.97	0.94
a facility and cheerful working enviroment.	4.03	0.94
a positive working environment.	4.13	0..83
Economic **I perceived that my organisation is able to: -**		
grow in sales.	4.12	0.91
grow in profitability.	3.91	0.91
increase return on equity.	3.97	0.94
increase in current ration.	4.03	0.94
sustain organisation performance	4.13	0..83
Quality Life of the Employees **I perceived that my organisation is able to: -**		
improve job satisfaction rate.	4.08	0.64
improve worker’s knowledge and awareness of insider threat.	4.29	0.75
improve the time quality between employers and employees.	4.17	0.74
improve financial analytic skills.	4.27	0.78
award recognition and bonus for employees.	4.25	0.85

Result

The first step conducted in the SEM analysis was Confirmatory Factor Analysis (CFA). CFA was utilized to identify individual constructs and was employed for three major purposes: (i) assessing model fit, (ii) establishing convergent validity, and (iii) confirming construct validity. Maximum likelihood estimation (MLE) was used to estimate the structural model.

The study adopted a two-step approach for modeling and analyzing the structural model, comprising Confirmatory Factor Analysis (CFA) and Structural Equation Modeling (SEM). Before modeling the structural model and executing SEM, it was essential to validate all measurement models of latent constructs for unidimensionality, validity, and reliability (Awang, 2014, 2015; Awang et al., 2015, 2017, 2018; Afthanorhan et al., 2017, 2018, 2019; Asnawi et al., 2019; Rahlin et al., 2019). This validation procedure is known as Confirmatory Factor Analysis (CFA).

A latent construct is considered valid (satisfying construct validity) if the fitness indexes achieved the three model fit categories: Absolute Fit, Incremental Fit, and Parsimonious Fit (Yusof et al., 2017; Mohd Azli et al., 2017; Awang et al., 2018; Rahlin et al., 2019; Asnawi et al., 2019; Shkeer & Awang, 2019). The fitness indexes and their respective threshold values are presented in Table 1.

Table 1
The three categories of model fit and their level of acceptance

Name of category	**Name of index**	**Level of acceptance**
Absolute Fit Index	RMSEA	RMSEA < 0.08
	GFI	GFI > 0.85 (ideal > 0.90)
Incremental Fit Index	AGFI	AGFI > 0.85 (ideal > 0.90)
	CFI	CFI > 0.85 (ideal > 0.90)
	TLI	TLI > 0.85 (ideal > 0.90)
	NFI	NFI > 0.90
Parsimonious Fit Index	Chisq/df	Chi-Square/ df < 5.0 (ideal < 3.0)

***The indexes in bold are recommended since they are frequently reported in literatures
Source: Awang (2015) and Awang et al. (2018).

The Measurement Model for Actor Characteristic Construct
The Actor Characteristics construct is a second order construct and this construct is measuredby the following five components namely:

1. SSSO (with 7 measuring items in a questionnaire)
2. MTAA (with 4 measuring items in a questionnaire)
3. PS (with 3 measuring items in a questionnaire)
4. HB (with 4 measuring items in a questionnaire)
5. IPC (with 5 measuring items in a questionnaire)

The measurement model for Actor Characteristics construct in IBM SPSS AMOS 25.0 is presented Figure 2.

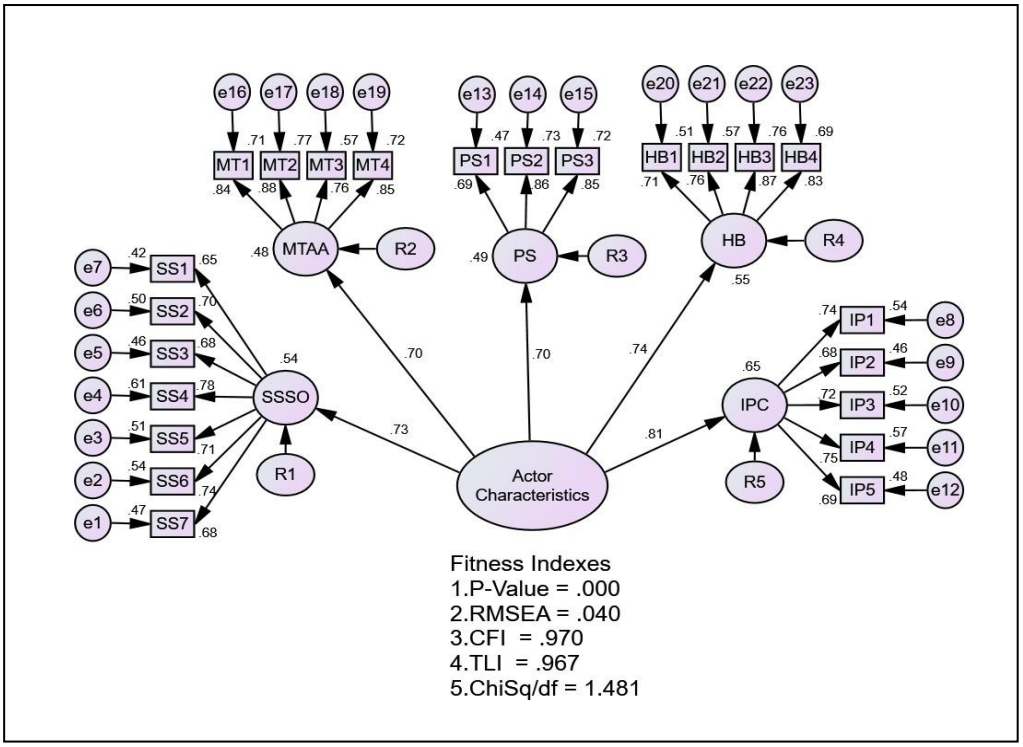


Figure 2: The CFA Result for Actor Characteristics construct

The study assessed **Convergent Validity** using **Average Variance Extracted (AVE)**. A construct is valid if its **AVE exceeds 0.5**, meaning it explains at least **50% of the variance** in its indicators (Awang, 2014, 2015; Aimran et al., 2017; Afthanorhan et al., 2017, 2018, 2019). For **Composite Reliability (CR)**, the study ensured that **CR values exceeded 0.6**, confirming that the indicators consistently measure the same construct (Awang, 2015; Awang et al., 2015, 2018).

Both **AVE and CR** results are presented in **Table 2**, verifying the reliability and validity of the measurement model. Additionally, model fit was assessed using:

- **Absolute Fit Indices:** Chi-square (χ^2), **RMSEA**, and **SRMR**, which measure how well the model fits the data.
- **Incremental Fit Indices: CFI** and **TLI**, which compare the model's fit to a baseline model.

These metrics confirm the accuracy and robustness of the measurement model.

The thorough assessment of these indices and their adherence to threshold values underscoresthe validity and reliability of the constructs within the model, ensuring accurate representationand meaningful interpretations of the research findings.

Table 2
The Average Variance Extracted (AVE) and Composite Reliability (CR)

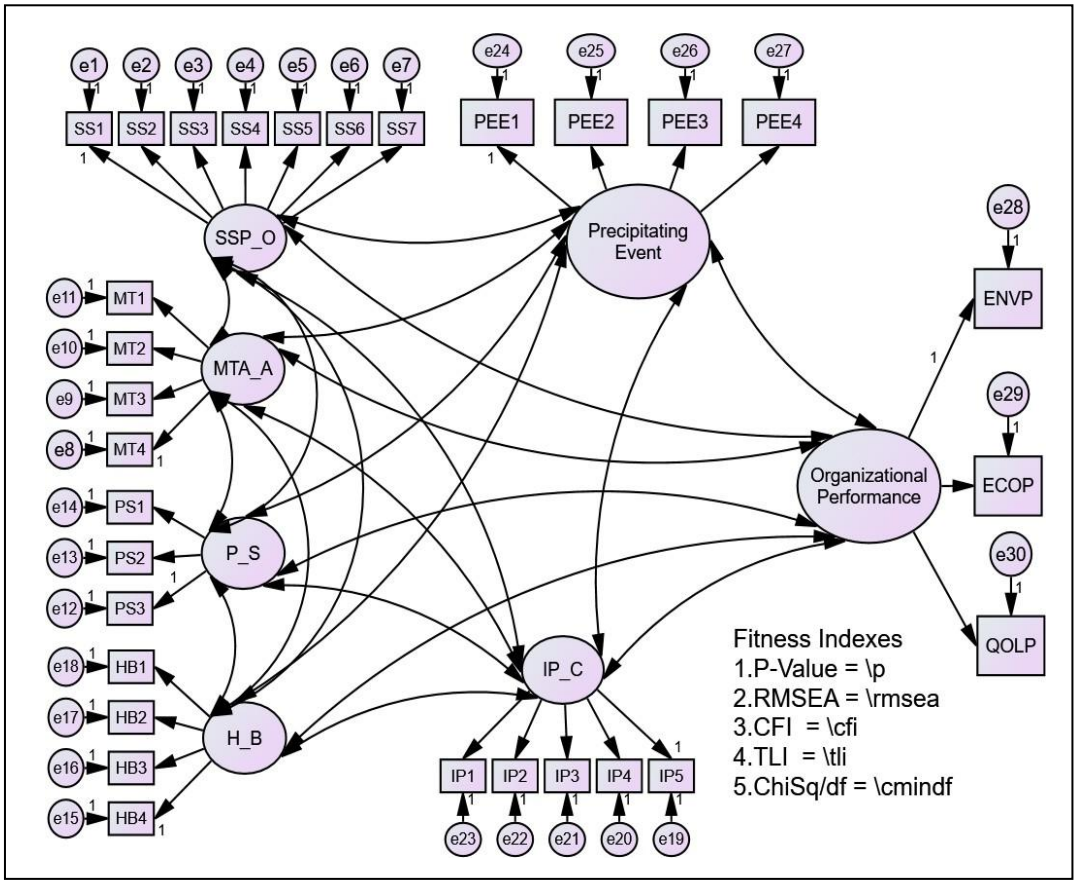
Construct	**Item**	**Factor Loading**	**CR (above 0.6)**	**AVE (above 0.5)**
Actor Characteristics	SSSO	0.73	**0.856**	**0.543**
	MTAA	0.70		
	PS	0.70		
	HB	0.74		
	IPC	0.81		
Component				
SSSO	SS1	0.65	**0.883**	**0.521**
	SS2	0.70		
	SS3	0.68		
	SS4	0.78		
	SS5	0.81		
	SS6	0.74		
	SS7	0.68		
MTAA	MT1	0.84	**0.901**	**0.695**
	MT2	0.88		
	MT3	0.76		
	MT4	0.85		
PS	PS1	0.69	**0.844**	**0.646**
	PS2	0.86		
	PS3	0.85		
HB	HB1	0.71	**0.872**	**0.632**
	HB2	0.76		
	HB3	0.87		
	HB4	0.83		
IPC	IP1	0.74	**0.840**	**0.543**
	IP2	0.68		
	IP3	0.72		
	IP4	0.75		
	IP5	0.69		

Based on the **Average Variance Extracted (AVE) and Composite Reliability (CR)** values in **Table 4**, the study confirms that the measurement model meets the requirements for **Convergent Validity and Composite Reliability** (Awang, 2014, 2015; Awang et al., 2018).

The **Confirmatory Factor Analysis (CFA)** results, illustrated in **Figure 2** and detailed in **Figure 3**, further validate the constructs' reliability and validity. These constructs are evaluated based on:

- **Construct Validity** – Assessed through fitness indices to ensure the model accurately represents theoretical constructs.
- **Convergent Validity** – Verified through **AVE**, confirming that the constructs effectively converge.
- **Discriminant Validity** – Evaluated using the **Discriminant Validity Index Summary** to ensure constructs remain distinct.

By adhering to these validation procedures, the study ensures the model is both **reliable and valid**, providing a strong foundation for further analysis (Awang, 2014, 2015; Awang et al., 2018; Rahlin et al., 2019; Asnawi et al., 2019; Mahfouz et al., 2019).



Figures 3: The CFA for all components of Actor Characteristics

Table 3
The Hypothesis Testing for Direct Effect Hypothesis

	Direct Effect Hypothesis	Result
H1a	**SSPO** has significant influence on **Precipitating Event**	Supported
H1b	**MTAA** has significant influence on **Organizational Performance**	Supported
H1c	**PS** has significant influence on **Precipitating Event**	Supported
H1d	**HB** has significant influence on **Precipitating Event**	Not Supported
H1e	**IPC** has significant influence on **Precipitating Event**	Supported

Conclusion

Insider threats are among the most challenging security concerns for organizations of all sizes, particularly in the industrial sector, which is the focus of this study. Numerous studies have been conducted in this field, and efforts continue to grow, though the boundaries and descriptions of insider threats remain somewhat ambiguous. Thus, understanding and gaining insights into insider threat detection is a crucial research direction. This paper aims to provide a comprehensive view and deep understanding of the characteristics of insider threats by surveying and categorizing the existing literature.

By deeply investigating the existing literature and analyzing real cases, this study delineates two distinct classes: insider threats and insider threat drivers. Significant information was obtained through an intensive literature review and analyzed data from a

real survey. This paper serves as a valuable reference for researchers by offering insights and organizing knowledge about insider threats.

The primary objective of this research is to assess the potential characteristics associated with insider threat drivers, combining both individual characteristics and precipitating events, to evaluate their impact on organizational performance. Utilizing a prototype psychological model, this research can provide crucial insights for government, industry, organizations, and employers to pre-emptively mitigate potential insider threats. Furthermore, it proposes a framework for further analysis and development of insider threat models and theories.

In addition to identifying and understanding insider threat characteristics, another crucial factor for organizations to consider in defending against these threats is the implementation of employee screenings. While not necessary for every organization, those that need to protect proprietary information may benefit significantly from screening and re-screening employment applicants and current employees. As Cummings et al. (2012) point out, screenings "help organizations to determine the trustworthiness of potential employees." Knowing an applicant's past can help identify potential future insider threats to the organization.

Organizations should also consider frequent re-screenings of current employees in positions of trust (Cummings et al., 2012). Although pre-employment screenings might initially prove employees to be trustworthy hires, life stressors can develop post-employment that place employees in difficult positions. Re-screenings can be particularly useful in identifying these stressors early and providing employees with help before they become insider threats (Cline, 2016).

Theoretical and Contextual Contribution

This study makes a significant theoretical contribution by refining the conceptual understanding of insider threat drivers through an integrated model incorporating actor characteristics, precipitating events, and organizational performance. By synthesizing multiple theoretical frameworks, including Social Bond Theory (SBT) and the Theory of Planned Behaviour (TPB), this research extends the literature on cybersecurity threats by demonstrating the interplay between individual behavioral traits and organizational vulnerabilities. The introduction of a validated Insider Threat Drivers (ITD) framework provides a structured mechanism for assessing insider threats, contributing to the advancement of threat mitigation strategies in academic and practical domains.

Contextually, this research is particularly relevant to Malaysia's cybersecurity landscape, addressing insider threats within the nation's manufacturing and industrial sectors. Given the increasing economic impact of cyber incidents in Malaysia, as highlighted by past data breaches and security violations, the findings offer organizations actionable insights to enhance their security protocols. By linking insider threat mitigation to organizational performance, this study emphasizes the practical significance of security measures in maintaining business continuity and protecting critical information assets. The research also highlights the role of employee training, ethical awareness, and technological

interventions in safeguarding organizations, thereby offering policymakers and industry leaders a comprehensive roadmap for strengthening cybersecurity resilience.

Insider Threats in Malaysia: Cases, Technology, and Mitigation

Insider threats remain a critical concern for organizations in Malaysia. In 2021, a major telecommunications company experienced a data breach due to an insider threat, exposing millions of personal records. Similarly, in 2019, a financial institution employee leaked customer data for financial gain, highlighting the vulnerabilities in the financial sector. These cases underscore the need for stronger security measures, including strict access controls and continuous monitoring.

Advancements in AI-driven behavioral analytics and machine learning have significantly enhanced insider threat detection. These technologies analyze user behavior, identify anomalies, and flag suspicious activities in real time, enabling proactive intervention. Automation reduces reliance on manual monitoring, minimizing risks posed by human error. Beyond technology, fostering a strong security culture is crucial. Employees who feel valued and engaged are less likely to become security risks. Regular cybersecurity training, ethical awareness programs, and transparent policies reinforce the importance of data protection. Creating a workplace that promotes trust and accountability can deter insider threats.

A comprehensive approach combining technology, strict policies, and employee engagement is essential to mitigating insider threats in Malaysia. By integrating these strategies, organizations can better safeguard their assets and enhance long-term cybersecurity resilience.

Acknowledgement

The researchers would like to express our gratitude to the Ministry of Higher Education (KPT) for sponsoring this study under the research grant TRGS/1/2016/PBPI-CITED/02/D00004. We would also like to thank Universiti Teknikal Malaysia Melaka for the opportunities given to us during this project period.

References

Clark, J. W. (2016). Threat from within: Case studies of insiders who committed information technology sabotage. Proceedings of the 11th International Conference on Availability, Reliability and Security, ARES 2016, 414–422. https://doi.org/10.1109/ARES.2016.78

Cline, H. G. (2016). Understanding the insider threat.

Colwill, C. (2010). Human factors in information security: The insider threat - Who can you trust these days? Information Security Technical Report, 14(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

Costa, D. (2017, March 7). CERT definition of 'insider threat' - Updated. [Blog post]. Retrieved from http://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). Insider threat study: Illicit cyber activity involving fraud in the U.S. financial services sector. Carnegie Mellon University, Software Engineering Institute, CERT Division.

DOSM. (2020). Department of Statistics Malaysia Press Release: Index of Industrial Production, Malaysia.

Ford, J. L., & Backhoff, E. G. (2019). From data to decision: A plan for mitigating insider threats. Journal of Information Warfare, 18(1), 53-63.

Jones, A., & Ashenden, D. (2005). Risk management for computer security. Butterworth-Heinemann.

Liang, N. P. (2016). Characteristics of malicious insiders and their relationships with different threats.

Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. Proceedings of the Annual Hawaii International Conference on System Sciences, 2015-March, 3518–3526. https://doi.org/10.1109/HICSS.2015.423

Martinko, M. J., Gundlach, M. J., & Douglas, S. C. (2002). Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. International Journal of Selection and Assessment, 10(1-2), 36–50.

Neely, A. D., Adams, C., & Kennerley, M. (2002). The performance prism: The scorecard for measuring and managing business success. Prentice Hall Financial Times.

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterizing attacks. Proceedings of the IEEE Symposium on Security and Privacy, 214–228. https://doi.org/10.1109/SPW.2014.38

Ponemon Institute. (2018). The 2018 insider threat report. Retrieved from https://www.observeit.com/2018-insider-threat-report/

Sedek, M., & Mohd, C. K. N. C. K. (2025). Exploring Educators' Perception of and Readiness for Hybrid Flexible Learning in Technical and Vocational Education and Training (TVET) in Higher Education. Scientific Journal of King Faisal University: Humanities and Management Sciences.

Schulze, H. (2018). Insider Threat 2018 Report. Retrieved from https://www.readkong.com/page/insider-threat-2018-report-4204677

Verizon. (2020). Breach investigations report. Retrieved from https://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf