International Research Journal of Multidisciplinary Scope (IRJMS), 2024; 5(4): 187-200 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2024.v05i04.01436

Malaysia's Insider Threat Risk: Developing a Tool

Nur Fahimah Mohd Nassir[1], Ummul Fahri Abdul Rauf[2]*, Zuraini Zainol[3], Asyraf Afthanorhan[4]

[1]Department of Defense Science, National Defense University of Malaysia. [2]Department of Mathematics, National Defense University of Malaysia, [3]Department of Computer Science, National Defense University of Malaysia, [4]Artificial Intelligence for Sustainability and Islamic Research (AISIR), Universiti Sultan Zainal Abidin. *Corresponding Author's Email: ummul@upnm.edu.my

Abstract

Insider threats pose significant challenges for organizations, causing severe financial and reputational damage. This study aims to develop a tool for measuring human, technical, and organizational factors contributing to insider threat risk levels in Malaysia's information and communications technology (ICT) sectors. We examined 40 items across these factors, validated by experts for content and criterion validity. We conducted a pre-test, adjusted based on expert feedback, and conducted a pilot study with 110 respondents from government agencies, ICT companies, and public tertiary institutions in Malaysia. Using IBM Statistical Package for Social Sciences, version 25.0, we performed exploratory factor analysis and tested the data with Bartlett's Test of Sphericity and Kaiser-Meyer-Olkin sampling adequacy tests. Cronbach's alpha assessed item reliability. The EFA grouped fifteen human factor items into three components: personal problems, negative personality traits, and inadequate security training. Four technical factor items formed one component, while fifteen organizational factor items split into issues with organizational practice, inadequate risk management, and ineffective management systems. Six insider threat risk level items formed a single component. Bartlett's Test of Sphericity was highly significant (Sig. < 0.001), and KMO values for all constructs exceeded 0.7, indicating excellent sampling adequacy. The overall Cronbach's alpha value for 40 items was 0.97, confirming the instrument's consistency and stability. These findings provide a reliable tool for predicting insider threat risk levels in Malaysia's ICT sectors, useful for researchers and practitioners alike.

Keywords: Cyber Security, Exploratory Factor Analysis, Insider Threat, ICT, Multidimensional.

Introduction

In an era dominated by digitalization and interconnected systems, the security of information and data has become paramount, particularly within the information and communications technology (ICT) sectors. Amidst this landscape, insider threats have emerged as a significant concern, posing risks to government organizations, businesses, and institutions globally, including Malaysia (1). Insider threats, which stem from individuals within the organization who exploit their access privileges to compromise data security, can have detrimental effects on confidentiality, integrity, and the availability of sensitive information. According to the Ponemon Institute's report (2), insider-caused incidents have increased, with 67% of businesses experiencing between 21 and 40 incidents annually. This is higher than the percentages in 2018 and 2020, which were 53% and 60%, respectively. Such threats can result in substantial financial loss, operational disruptions, and severe reputational damage (3). As depicted in Figure 1, insider threats have classified these risks into two broad categories: intentional and inadvertent insider threats. Intentional insider threats involve individuals who deliberately exploit their access to sensitive information for harmful purposes, such as cyber espionage or sabotage. These individuals may be motivated by financial gain (4), disgruntlement (5), or coercion by external actors (6). In contrast, inadvertent insider threats arise from unintentional actions that result in security breaches, typically due to negligence (7), lack of awareness (8), or inadequate risk assessment (9). Common examples include accidental publishing of sensitive information, configuration errors, or improper encryption practices (10). Even though these insiders have no malicious intent, their actions can create vulnerabilities that malicious actors can exploit.

(Received 25th June 2024; Accepted 17th October 2024; Published 30th October 2024)

Furthermore, a report from MyCERT on cybercrime incidents in 2023, as illustrated in Figure 2, reveals that Malaysia recorded over 5,917 cyber security incidents, with the majority involving fraud (3,705 incidents), intrusion (508 incidents), and malicious codes (509 incidents). While external threats like intrusions and malware remain significant concerns, the growing impact of insider actions, both intentional and inadvertent, has become increasingly evident in these reported cases. Insider threats, such as negligence, misuse of privileges, and malicious intent, frequently evade traditional cyber security defenses, making them particularly challenging to detect and address. The lack of adequate insider threat management may be contributing to the upward trend in data breaches, facilitating the occurrence of fraud and other cyber incidents (11).

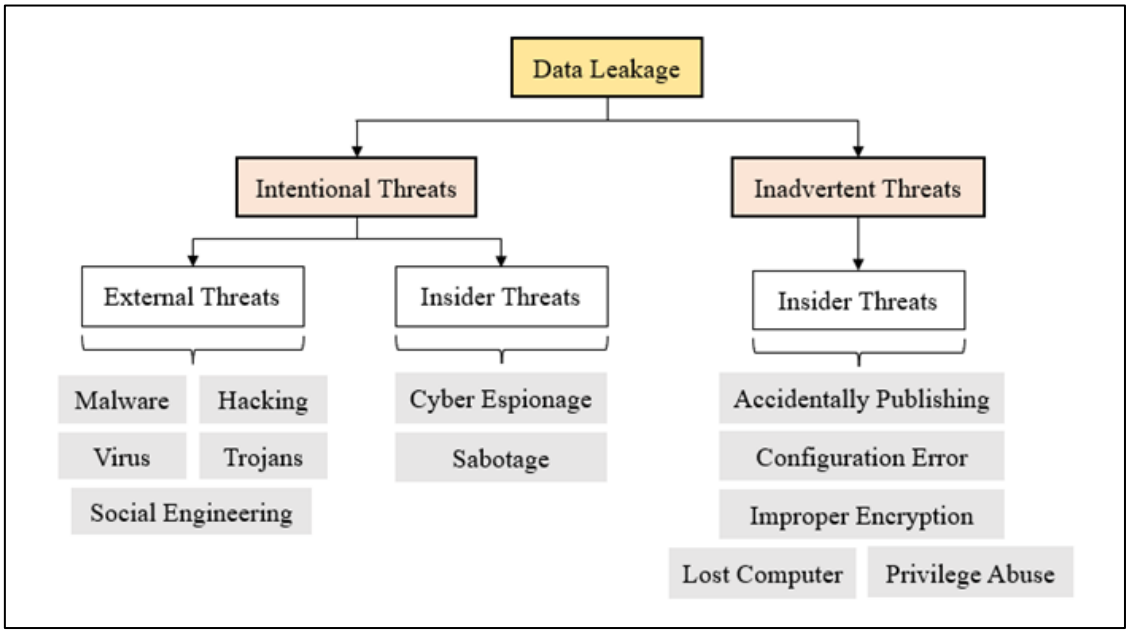

Figure 1: Classification of Enterprise Data Leak Threats

#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Denial of Service	0	1	2	4	0	1	1	2	4	8	2	0	25
Intrusion	72	39	46	30	39	37	84	49	23	29	43	17	508
Content Related	12	37	53	45	51	50	58	72	62	66	79	61	646
Intrusion Attempt	22	17	17	15	26	27	38	23	23	66	49	31	354
Vulnerabilities Report	10	9	9	2	3	7	5	6	2	2	8	28	91
Malicious Codes	24	45	71	62	57	41	32	27	38	43	32	37	509
Fraud	235	222	340	338	374	290	279	322	388	299	360	258	3,705
Spam	13	6	5	4	6	9	5	9	4	4	9	5	79
	388	376	543	500	556	462	502	510	544	517	582	437	5,917

Figure 2: Malaysia's Incidents of Cybercrime Reported in 2023

As a result, these unique challenges posed by insider actions underscore the importance of addressing these risks through specialized tools and strategies tailored to the specific vulnerabilities of the sector. In particular, the ICT sectors in Malaysia serves as a critical reference point for addressing cybersecurity issues across other sectors, including national defense, financial systems, healthcare, and government operations (12). Thus, any vulnerability within the ICT sector can have cascading effects across the broader economy. Therefore, to effectively mitigate insider threats across all sectors, it is essential to first focus on understanding and addressing these risks within Malaysia's ICT sector. Furthermore, this sector remains vulnerable to these threats, even more so than external cyberthreats. Given the critical nature of the ICT infrastructure, this study acknowledges the critical need to proactively address insider threats by developing a tailored instrument to measure insider threat risk levels specific to Malaysia's ICT sectors. In 2014, the development of the Insider Threat Indicator Ontology (ITIO) marked a significant advancement in this direction. Its main purpose is to find behavioural and technical indicators of malicious insider activity (13, 14). This ontology primarily relies on resources, such as the compilation of insider threat cases from Management and Enterprise Risk Intelligence Tool (MERIT) database, which catalogues various incidents of insider threats, including fraud, sabotage, and theft of intellectual property. While earlier models have addressed human behavioural factors within structured frameworks of insider threat risk, the Sociotechnical and Organizational Factors for Insider Threat (SOFIT) later proposed a structural model emphasising individual and organisational sociotechnical factors, integrating technical indicators from prior research (9). Additionally, in 2020, the Insider Threat Risk Prediction framework was introduced, which employs a multi-perspective approach to anticipate malicious insider threats before they occur (15). More recently, Min Zeng, Chuanzhou Dian, and Yaoyao Wei emphasised the importance of exploring key human factors to effectively prevent insider threats, enhancing their framework by incorporating human factors (16). According to a report from the Software Engineering Institute, effectively managing insider threats requires a coordinated strategy that encompasses human, technical, and organisational factors (17).

Upon reviewing the existing literature, it is evident that while research on insider threats is growing, there remains a gap in the development of comprehensive instruments and methodologies specifically tailored to address the problem from multiple perspectives, encompassing both malicious and unintentional insiders. Additionally, existing studies have predominantly focused on conceptual frameworks and case studies from other regions, underscoring the necessity for localised research and solutions. There is a need for more research that considers the unique cultural and organisational contexts of Malaysia. Motivated by this identified gap in the literature, the primary objective of this study is to develop a multidimensional instrument that can effectively measure insider threat risk levels within Malaysia's ICT sectors. By conducting a thorough exploration of the factors contributing to insider threats through leveraging insights from existing literature and Exploratory Factor Analysis (EFA), we aim to develop a comprehensive and contextually relevant instrument that can assist organisations in mitigating this critical security risk effectively. Through this research endeavour, we aspire to contribute to the body of knowledge on insider threat management by providing a validated tool that measures the relevant risk factors comprehensively. The findings from this study are expected to aid organisations in implementing more effective insider threat mitigation strategies, ultimately fostering a safer and more resilient digital ecosystem.

Methodology

This study developed a tool that adheres to the requirements of structural equation modelling (SEM) and includes four key constructs: the human factor (HF), the technical factor (TF), the organisational factor (OF), and the insider threat risk levels (ITRL). Initially, the development was based on a theoretical framework (15) that encompasses human, technical, and organisational factors, though it was originally limited to addressing only malicious insiders. Furthermore, we expanded the framework to include both intentional and inadvertent insider threats, acknowledging the need for a more inclusive approach. We conducted a content analysis of previous studies on insider threats to identify a broader range of contributing factors, such as human behaviours, technical vulnerabilities, and organisational weaknesses. Following this, we refined the factors identified

through expert consultations with cybersecurity professionals and academic researchers, whose insights ensured that the tool not only reflected theoretical knowledge but also had practical relevance. This iterative process allowed us to enhance the tool's applicability, ensuring it addresses both intentional and inadvertent insider threats from a comprehensive perspective. Additionally, a rigorous series of validation steps, including expert validation, pre-testing, pilot testing, and EFA, was undertaken to ensure the tool's reliability and accuracy in measuring insider threat risks.

Instrument

This study employed an online self-administered survey questionnaire, consisting of 40 closed-ended questions, to collect insights from the target population in Malaysia's ICT sectors. The survey aimed to identify the factors influencing insider threat occurrences and assess the impact of these threats. We presented these 40 items, designed to measure insider threat risk levels, on a 10-point interval scale, ranging from "1 = strongly disagree" to "10 = strongly agree". The 10-point interval scale provides respondents with more response options, allowing for more precise judgments of given statements (18). We developed the items by analyzing previous studies' content, specifically tailoring them to the context of our investigation to assess insider threat risk levels within Malaysia's ICT sectors. Table 1 displays the construct we used to measure insider threat risk levels.

Table 1: Construct and Item Numbers of Insider Threat Risk Levels Variable

Construct	Number of the Item	Item Numbers
Human Factor	15	H1 – H15
Technical Factor	4	T1 – T4
Organisational Factor	15	O1 – O15
Insider Threat Risk Levels	6	IT1 – IT6

Expert Validation

Experts in the field comprehensively evaluated the items in the questionnaire for validity and reliability. Validity refers to the degree to which a score accurately represents a concept, whereas reliability of the questionnaire can be defined as the capacity to consistently generate the same result across time and among different observers (19). Expert validation, encompassing face validity, content validity, and criterion validity, comprises three forms of validity evaluation aimed at assessing the reliability and effectiveness of the instrument. These steps are essential in validating the extent to which the survey instrument accurately measures its intended purpose (20). For this study, content and criterion validity are applied. Specifically, content validity refers to how accurately the items or tests within a measurement instrument represent the behavior under study (21), while criterion validity evaluates the degree of correlation between a measure and other recognized measures for the same construct (22). Five experts, including professors and associate professors in the fields of social sciences, statistics, and cybersecurity, evaluated the items. Furthermore, the statistical expert assessed the instrument's measuring scale criterion validity, which met the requirement for parametric statistical analysis. The researcher requested the experts assess the language used, comprehensibility, appropriateness, item's clarity, sufficiency of items to measure the constructs, and overall questionnaire arrangement. The experts provided feedback and comments on the instrument. Based on their feedback and suggestions, statements were revised accordingly.

Pre-Test

We conducted a pre-test after modifying the questionnaire to ensure that the instrument items were suitable for research objective and easy to comprehend (23). During the pre-test phase, the questionnaire underwent review and examination by seven external experts and practitioners to validate its accuracy and ensure alignment with the research objectives. Pre-testing involved four senior cybersecurity officers from the Malaysian Armed Forces (MAF) and three academicians specializing in cybersecurity, statistics, and computer science. Their feedback helped to improve the instrument's competency level. The researcher selected the experts and practitioners using a judgment sampling method, considering their expertise as subject matter experts (SMEs) in ICT sectors and their ability to provide clear explanations and suggestions for improvement. Judgment sampling is the process of selecting sample members based solely on

the researcher's knowledge and best judgment (24). We conducted the pre-test by distributing the questionnaire to the reviewers online. We asked the reviewers to provide feedback on various aspects of the questionnaire, such as its format, wording, sequence, and clarity. The researcher collected their comments and suggestions and modified the instrument, accordingly, thereby improving its quality. Following these adjustments, a new version of the questionnaire was introduced.

Pilot Test

Once the pre-testing phase is complete, a pilot test is performed as a small-scale study, utilising study participants selected from the actual target population. This pilot study seeks to ensure that the characteristics of the study sample closely mirror those of the population, identify any shortcomings in the study instrument, and produce initial findings regarding the adequacy of the study hypothesis. It is necessary to conduct pilot testing in order to validate the modified instrument (25-29). This is of utmost importance, particularly if the preceding instrument was tailored for a distinct cultural and industrial population than that of this study (30). During this phase, there are two government agencies, two Malaysia's ICT enterprise companies, and one public university offering ICT course in Kuala Lumpur were selected for this study based on their fulfilment of specific criteria. For the EFA, a minimum sample size of 100 was recommended to obtain valid results (31). In this study, questionnaires were distributed to a total of 115 respondents, selected using simple random sampling. This method ensured that each member of the target population had an equal chance of being chosen, making the results generalizable. However, five questionnaires were excluded due to irrelevant responses that did not align with the research objectives. Therefore, the final number of questionnaires analysed was 110.

Exploratory Factor Analysis (EFA) Procedure

Social science research typically employs two primary methodologies for factor analysis: EFA and confirmatory factor analysis (CFA). It is customary to conduct an EFA before proceeding to a CFA (32). The EFA statistical technique explores and evaluates the utility of each measuring item, identifying its underlying dimensions. Through factor extraction, rotation, and interpretation, EFA provides a systematic approach to understanding the relationship among variables and uncovering hidden patterns in the data. In our study, EFA played a pivotal role in identifying and organising the different groups of questions in our measurement tool, ensuring that each group accurately measures different aspects of human, technical, and organisational factors. Initially, EFA assisted us in analysing and refining the full set of questions we compiled, which aimed to assess these various factors. This refinement process involved evaluating the relevance and effectiveness of each question or statement, allowing us to adjust or remove those that did not clearly contribute to an understandable and concise grouping of factors. Furthermore, we were also able to confirm the reliability of these constructs by using EFA. This showed that the groups of items did, in fact, reflect different factors in the context of insider threat risk assessment. This validation was critical not only for theoretical alignment but also for the tool's practical application in effectively predicting and managing insider threats. Through this analytical process, we ensured that this tool could reliably differentiate between the nuances of the three key areas of risk, providing a solid foundation for further analysis and practical application in the field. For the purpose of this study, EFA approach recommended in the study was implemented (33). We utilised data gathered from a pilot study to conduct the EFA procedure, employing IBM-SPSS 25.0 software for the analysis. The Kaiser-Meyer-Olkin (KMO) test was employed to assess the adequacy of the sample size for analysis across all constructs. The following formula gives the KMO measure of sampling adequacy:

$$KMO_j = \frac{\sum_{i \neq j} R_{ij}^2}{\sum_{i \neq j} R_{ij}^2 + \sum_{i \neq j} U_{ij}^2} \quad \text{---------- [1]}$$

A KMO value greater than 0.50 (KMO ≥ 0.50) is considered suitable for refining measurement items (34). Table 2 presents specific KMO value ranges and significance grades.

Table 2: Summary of KMO Value Range

KMO Value Range	Grading
≥ 0.90	Excellent
0.80 – 0.90	Very good
0.70 – 0.80	Good
0.60 – 0.70	Moderate
0.50 – 0.60	Poor
≤ 0.60	Very poor

Additionally, Bartlett's sphericity test was utilised to measure the correlation that exists between variables or items and ascertain the suitability of the sample for factor analysis. The value of Bartlett's Test of Sphericity must be less than 0.05 (p-value < 0.05) for factor analysis to be acceptable. In order to measure the overall relationship between the variables, the determinant of the correlation matrix |R| is calculated. Under H0, |R| = 1; if the variables are highly correlated, then |R| ≈ 0. We calculate Bartlett's test of sphericity as follows:

$$X^2 = -\left(n - 1 - \frac{2p-5}{6}\right) \times ln\ ln\ |R| \quad \text{----------[2]}$$

The Eigenvalue of each factor, which must exceed 1.0, then determines its significance. We selected the varimax rotation method because it maximizes the variance loading in the matrix and enhances the clarity of factor separation.

After reviewing the guidelines on analysis type and sample size as recommended by the study (35), items with factor loading values of 0.60 or higher were retained within their respective constructs for further analysis. These items are considered practically significant and demonstrate a high level of acceptability. Conversely, we removed items with a factor loading below 0.60 and those that were redundant from the questionnaire. On the other hand, Cronbach's alpha was employed to assess the internal reliability of the instruments (36) and can be expressed as:

$$\alpha = \frac{n\underline{r}}{1+\underline{r}\,(n-1)} \quad \text{----------[3]}$$

The value of Cronbach's alpha should be greater than 0.70 for the items to achieve internal reliability, which shows the effectiveness of a set of items in measuring, constructs (37). In summary, the researcher has meticulously adhered to the established methodology to guarantee the use of high-quality, robust instruments that align with the culture of Malaysia's ICT sectors.

Results and Discussion

EFA for Insider Threat Risk Levels

A total of 40 items were explored using the EFA procedure. The items represent four constructs: HF, TF, OF, and ITRL. The mean and standard deviation of every item in these four constructs are shown in the descriptive statistical result, as shown in Table 3.

Table 3: Descriptive Analysis for Items Measuring Insider Threat Risk Levels

Construct	Item Label	Item Statement (I believe that...)	Mean	Standard Deviation (SD)
Human Factor	H1	A lack of information security knowledge may cause unintentional insider threat incidents.	8.54	1.663
	H2	Inadequate training on security policies and procedures may expose the organisation to insider threats.	8.61	1.421
	H3	Individuals who are dealing with deep frustration may increase the risk of insider threats.	8.05	1.822
	H4	Stressed employees may accidentally reveal confidential information.	7.97	1.794
	H5	Individuals with financial issues might purposely reveal confidential information for their own financial gain.	7.95	1.658
	H6	Drug addicts may intentionally or unintentionally reveal crucial data.	8.20	1.674

	H7	Individuals who have been blackmailed may do bad things unintentionally.	8.33	1.598
	H8	Unsatisfied individuals who feel unappreciated are likely to misuse sensitive information for revenge.	8.11	1.794
	H9	Individuals who have poor relationships with colleagues might lead to insider threat incidents.	7.56	1.779
	H10	Curiosity about confidential information by individuals may raise the risk of insider threats.	7.95	1.564
	H11	Careless individuals are more likely to expose sensitive information unintentionally.	8.45	1.554
	H12	Resistance behaviour to security practices may raise the risk of insider threats.	7.90	1.781
	H13	Playful individuals are more likely to engage in unintentional insider threat actions.	7.47	1.985
	H14	Disloyalty to the organisation could make individuals more likely to commit insider threats.	8.42	1.678
	H15	Greed may influence individuals to commit insider threats for their own benefit.	8.34	1.736
Technical Factor	T1	Weaknesses in infrastructure such as hardware, software, and networks can lead to insider threat incidents.	8.47	1.668
	T2	Insufficient technical monitoring tools could increase the risk of insider threats.	8.37	1.669
	T3	Insufficient system security testing and evaluation could increase the risk of insider threats.	8.34	1.715
	T4	Lack of proper vulnerability assessments on ICT infrastructure would increase the insider threat risk.	8.35	1.650
Organisational Factor	O1	Poor organisational culture may cause employees to ignore the processes, increasing insider attack risk.	8.23	1.811
	O2	Insider threats are more likely to occur when an organisation's security culture is lacking.	8.52	1.470
	O3	A high level of trust in certain employees may increase insider threat risk within the organisation.	7.78	2.078
	O4	Poor communication and collaboration among employees would increase the risk of an insider threat.	7.80	1.994
	O5	Lack of control over staff access could raise the risk of insider threats.	8.36	1.663
	O6	Insufficient incident response planning may encourage intentional insider threats.	8.16	1.795
	O7	Inadequate risk assessment can lead to more insider threat incidents.	8.05	1.696
	O8	Without a thorough background check during the hiring process, organisation may hire individuals who will commit insider threat.	8.35	1.679
	O9	A lack of individual behavior monitoring mechanisms may limit the ability to trace intentional threats.	8.31	1.537
	O10	Weaknesses in security policies and procedures may increase the likelihood of insider threats.	8.55	1.398

	O11	Data sharing flaws may make it easier for insider threats to occur.	8.49	1.537
	O12	Inadequate security awareness and training programmes organised by organisations may lead to insider attacks.	8.44	1.577
	O13	A lot of work can make people very tired, which might increase the risk of insider threats.	7.83	2.045
	O14	Working in a very stressful environment can lead individuals to engage in insider threats.	7.85	2.128
	O15	Unfair workloads make employees unsatisfied with their jobs and may raise the risk of insider threats.	8.01	1.865
	IT1	Organisation's reputation would be significantly damaged if an insider threat incident occurred.	8.48	1.624
	IT2	An incident involving an insider threat would cause the organisation to experience significant financial losses.	8.34	1.403
Insider Threat Risk Levels	IT3	An insider threat incident would severely damage the public's trust in that organisation.	8.72	1.376
	IT4	The risk of insider threats includes the potential theft of the organisation's intellectual property.	8.54	1.392
	IT5	Insider threat incidents could result in the loss or leakage of an organisation's critical data.	8.59	1.622
	IT6	Operational continuity could be severely affected by insider threats.	8.32	1.458

KMO and Bartlett's Test of Sphericity

The KMO values for HF, OF, and ITRL are 0.886, 0.890, and 0.889, respectively. These values exceed the required value of 0.8, indicating excellent adequacy. The TF exhibits a KMO value of 0.797, which is also acceptable. These findings suggest that the data is sufficient to proceed with the data reduction procedure in EFA. Bartlett's Test of Sphericity produces results that are highly statistically significant (Sig. < 0.001). In addition, the KMO values for sampling adequacy are considered good to excellent, as shown in Table 4.

Table 4: The KMO and Bartlett's Test Value

		Human Factor	Technical Factor	Organisational Factor	Insider Threat Risk Levels
Kaiser-Meyer-Olkin measure of Sampling Adequacy		**0.886**	**0.797**	**0.890**	**0.889**
Bartlett's Test of Sphericity	Approx. Chi-Square	1032.161	343.305	1180.074	387.811
	df	105	6	105	15
	Sig.	**.000**	**.000**	**.000**	**.000**

Total Variance Explained

All of these components have Eigenvalues greater than 1.0. The variance values show that the HF construct accounts for 68.04%, the TF for 81.61%, the OF for 70.97%, and the ITRL for 68.36%. This indicates that the number of components and items for each construct is appropriate, as the total variance for each construct exceeds 60% (38). The findings in Table 5 demonstrate that the HF construct consists of three components, the TF construct consists of one component, the OF construct consists of three components, and the ITRL construct consists of one component.

Table 5: The Total Variance Explained for Each Construct

Construct	Comp	Extraction Sums of the Squared Loadings			Rotation Sums of Squared Loadings		
		Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
Human Factor	1	7.368	49.121	49.121	3.894	25.961	25.961
	2	1.494	9.959	59.079	3.624	24.158	50.119
	3	1.345	8.967	68.046	2.689	17.927	68.046
Technical Factor	1	3.265	81.615	81.615	-	-	-
Organisational Factor	1	7.790	51.930	51.930	3.854	25.693	25.963
	2	1.878	12.520	64.450	3.589	23.928	49.621
	3	.978	6.522	70.972	3.203	21.351	70.972
Insider Threat Risk Levels	1	4.102	68.365	68.365	-	-	-

Scree Plot

To determine whether the eigenvalue is sufficiently high to indicate a significant factor, one technique is to plot a graph, known as a scree plot. The graph displays each eigenvalue on the Y-axis against the corresponding factor on the X-axis, highlighting significant factors. Figure 3 displays a scree plot illustrating the emergence of three components generated by the EFA procedure for the HF construct. 15 items were grouped into three components: component 1 for personal problems, component 2 for negative personality traits, and component 3 for inadequate security training. Additionally, the scree plot for the TF construct combined four items into one component, as shown in Figure 4. Figure 5 illustrates the OF construct. They sorted 15 items into three components, and they named component 1 for organisational practice issues, component 2 for inadequate risk management, and component 3 for ineffective management systems.

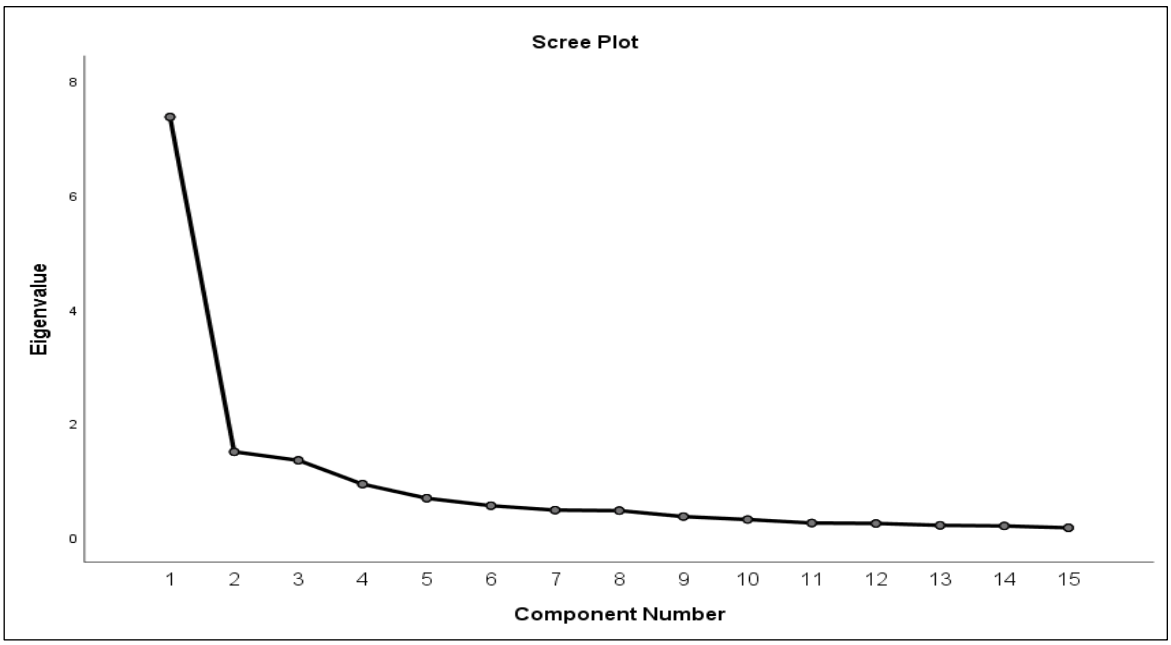

Figure 3: Scree Plot of the Human Factor Construct

Figure 4: Scree plot of the Technical Factor Construct

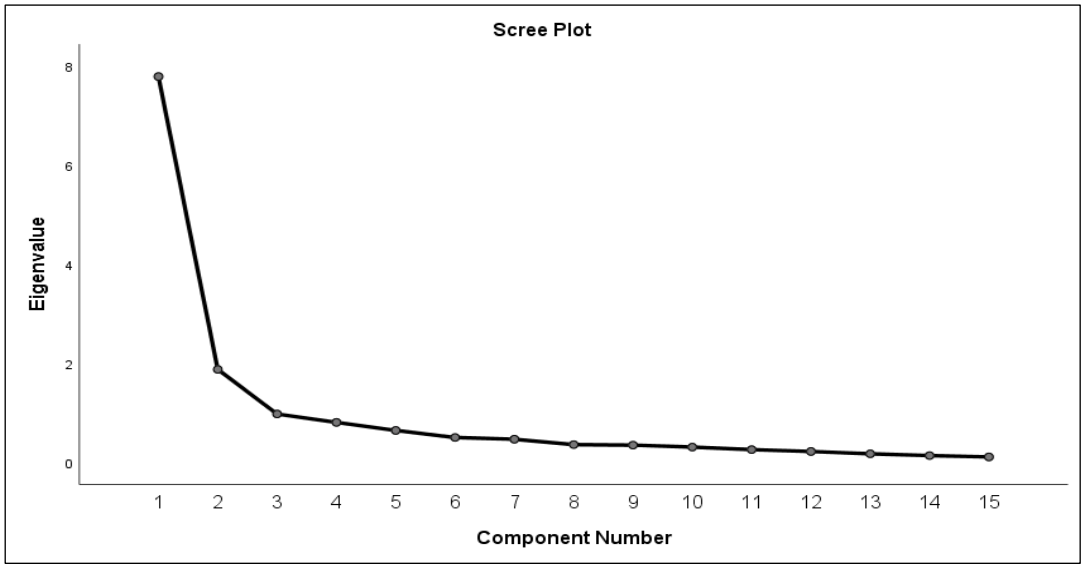

Figure 5: Scree Plot of the Organisational Factor Construct

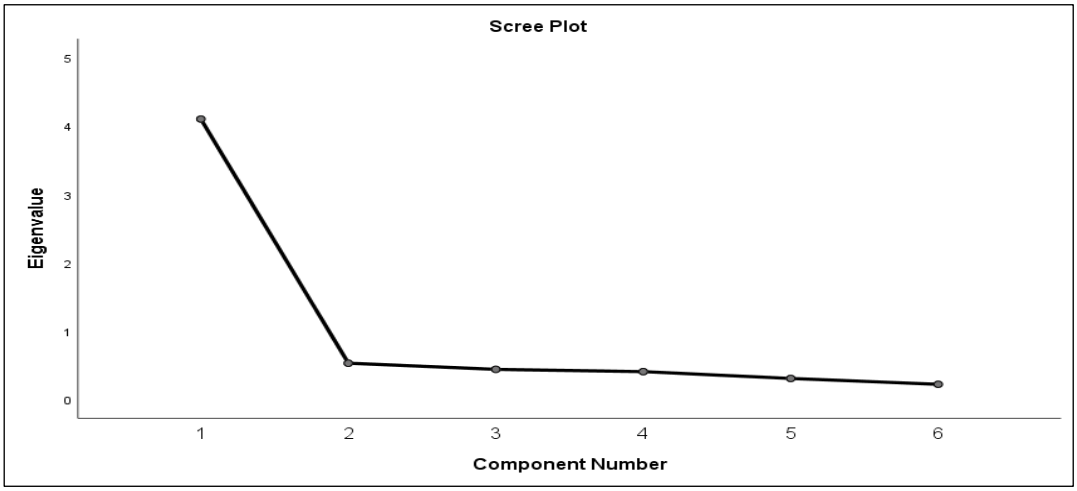

Figure 6: Scree Plot of the Insider Threat Risk Levels Construct

Subsequently, the ITRL construct grouped six items into one component, as shown in Figure 6. The rotated component matrix dictates which items are associated with which component (29). These results highlight the clarity and effectiveness of the factor analysis in organising the items within each construct.

Rotated Component Matrix

After determining the total variance for each construct, the next step involves determining the number of items for each individual component. The items for the HF construct were categorised into three components: personal problems, which consisted of seven items; negative personality traits, which contained six items; and inadequate security training, which loaded two items. We retained 13 of 15 items because their factor loading was above 0.6, and excluded 2 due to their impoverished factor loading. We need to omit components H6 and H10. Table 6 depicts the rotated component matrix for the HF construct.

Table 6: Rotated Component Matrix for Human Factor

Comp	Item Label														
	H1	**H2**	**H3**	**H4**	**H5**	**H6**	**H7**	**H8**	**H9**	**H10**	**H11**	**H12**	**H13**	**H14**	**H15**
1			.755	.845	.715	.562	.762	.660	.613						
2										.590	.663	.794	.728	.603	.626
3	.848	.802													

Table 7: Rotated Component Matrix for Technical Factor

Comp	Item Label			
	T1	**T2**	**T3**	**T4**
1	.902	.925	.888	.898

Table 8: Rotated Component Matrix for Organisational Factor

Comp	Item Label														
	O1	**O2**	**O3**	**O4**	**O5**	**O6**	**O7**	**O8**	**O9**	**O10**	**O11**	**O12**	**O13**	**O14**	**O15**
1		.608			.775	.802	.730	.608	.659						
2			.727	.635									.883	.881	.777
3	.693									.608	.851	.852			

For each item in the TF construct, the latent factor value exceeds 0.6. Therefore, there is no need to discard any items, as all items possess latent factor values that exceed the requirement of 0.6. Thus, Table 7 maintained all items as a single component. The EFA technique derived three components from 15 items, as shown in Table 8. The three components consisted of organisational practice issues, which encompassed six items; inadequate risk management, which comprised five items; and ineffective management systems, which included four items. We retained all items because their latent factor values exceeded 0.6. Otherwise, Table 9 displays that six items were placed into a single component and none of the items were removed because all of them are appropriate for evaluating the ITRL construct.

Table 9: Rotated Component Matrix for Insider Threat Risk Levels

Comp	Item Label					
	IT1	**IT2**	**IT3**	**IT4**	**IT5**	**IT6**
1	.840	.797	.853	.777	.858	.833

Internal Reliability of Instrument

Internal reliability, also referred to as consistency, gauges the degree of interconnection among the items within a construct. Each construct's components have a Cronbach's alpha greater than 0.80. In addition, Cronbach's alpha value for all 40 items is 0.969, which also exceeded the threshold value of 0.80. Therefore, the study concluded that the instrument measuring

insider threat risk levels has adequate internal reliability (39). Table 10 presents the components for each construct, which measure human, technical, organisational factors, and insider threat risk levels, along with their respective Cronbach's alpha values.

Table 10: Cronbach's Alpha for Each Component

Construct	Comp	Number of items	Cronbach's Alpha
	1	6	0.895
Human Factor	2	5	0.827
	3	2	0868
Technical Factor	1	4	0.925
	1	6	0.892
Organisational Factor	2	5	0.895
	3	4	0.871
Insider Threat Risk Levels	1	6	0.907

Contribution

This study's primary contribution is the creation of a multidimensional tool that measures insider threat risk levels by incorporating human, technical, and organisational factors. This tool advances existing theories in cybersecurity, risk management, and organisational behaviour by providing a more comprehensive framework for understanding insider threats. Traditional cybersecurity theories have largely focused on specific perspectives, addressing only one or two dimensions, such as human, technical, or organisational factors, without integrating all three. By integrating these dimensions, the tool expands upon existing insider threat models, offering a more holistic approach to risk assessment. From a risk management perspective, this tool integrates multiple dimensions, advancing the field beyond traditional models that focus primarily on malicious insider. The tool offers a broader understanding of risks, often overlooked in existing theories, by addressing both intentional and inadvertent insider threats. Additionally, by providing a practical instrument to quantify insider threat risks and inform decision-making, the tool enhances risk management frameworks. For example, by identifying specific human, technical, and organisational components, organisations can customize their risk management strategies to address their most pressing vulnerabilities. This offers a significant improvement over traditional risk management models, which may overlook the complex interplay between these factors. In the context of organisational behaviour, the tool contributes to theories related to employee behaviour, organisational culture, and the role of internal policies in shaping insider threats. By addressing these dimensions, this study not only enhances theoretical understanding but also provides a practical tool that organisations can use to improve their insider threat detection and risk management strategies.

Conclusion

In this study, we successfully developed a multidimensional tool for assessing insider threat risk levels within Malaysia's ICT sectors, utilising EFA. The findings underscore the critical importance of addressing insider threats through a comprehensive approach that integrates human, technical, and organisational factors. By identifying these dimensions, organisations are better equipped to implement precise and targeted strategies to mitigate these risks effectively. Although this study achieved the development and initial validation of the tool using EFA, further steps are necessary to ensure its ongoing practical applicability within the ICT sectors. Future research will employ CFA to validate the factor structure identified during EFA and to confirm the robustness of the constructs across different contexts. This additional validation will provide a more nuanced understanding of how the identified factors perform in various sectors and environments, particularly in ICT settings, ensuring the tool's reliability and adaptability in real-world applications. Additionally, as artificial intelligence (AI) and machine learning (ML) technologies continue to be integrated into cybersecurity practices, future research may explore how these advancements could be incorporated into insider threat detection. While AI and ML offer the potential for enhanced detection capabilities by

identifying behavioural anomalies and predicting risks with greater accuracy, they also pose new challenges, such as the potential for insider manipulation of AI systems and biases in detection algorithms. Furthermore, overreliance on automation may reduce essential human oversight in managing insider threats. Therefore, the tool developed in this study could be adapted in the future to incorporate AI-driven indicators, ensuring its continued effectiveness while mitigating the potential risks associated with these emerging technologies.

Abbreviations

HF: Human Factor, TF: Technical Factor, OF: Organizational Factor, ITRL: Insider Threat Risk Levels, EFA: Exploratory Factor Analysis, Comp: Component.

Acknowledgement

Nil.

Author Contributions

Nur Fahimah Mohd Nassir: conceptualized the research, collected data, and contributed to data analysis and interpretation of findings; Ummul Fahri Abdul Rauf: led the data analysis, contributed to the interpretation of findings, and critically reviewed the manuscript; Zuraini Zainol: assisted in the research design, contributed to data collection, and reviewed and revised the manuscript content; Wan Mohamad Asyraf Wan Afthanorhan: provided statistical guidance for data analysis and reviewed the final manuscript.

Conflict of Interest

The authors declare that there is no conflict pertaining to this paper.

Ethics Approval

This study received ethical approval from Jawatankuasa Etika Penyelidikan (JKEP), National Defence University of Malaysia, with the clearance number 15/2023, dated November 8, 2023.

Funding

This study was supported by the Malaysian government under the Skim Pengajian Tinggi Tentera Darat (SPTTD).

References

1. Majlis Keselamatan Negara. Malaysia Cyber Security Strategy 2020-2024. The Government of Malaysia; 2020. p91.
2. Ponemon Institute. 2022 Cost of Insider Threats Global Report. Proofpoint; 2022. p45.
3. Kisenasamy K, Perumal S, Raman V, Singh BSM. Influencing factors identification in smart society for insider threat in law enforcement agency using a mixed method approach. International Journal of System Assurance Engineering and Management. 2022 Mar 1;13:236–51.
4. Mészáros AÁ, Kelemen-Erdős A. Industrial espionage from a human factor perspective. Journal of International Studies. 2023;16(3):97–116.
5. Sepehrzadeh H. A method for insider threat assessment by modeling the internal employee interactions. International Journal of Information Security. 2023 Oct 1;22(5):1385–1393.
6. Kisenasamy K, Perumal S, Raman V, Singh BSM. Influencing factors identification in smart society for insider threat in law enforcement agency using a mixed method approach. International Journal of System Assurance Engineering and Management. 2022 Mar 1;13:236–51.
7. Yeo LH, Banfield J. Human factors in electronic health records cybersecurity breach: an exploratory analysis. Perspectives in health information management. 2022;19(Spring).
8. Green ML, Dozier P. Understanding Human Factors of Cybersecurity: Drivers of Insider Threats. In: Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience, CSR 2023. Institute of Electrical and Electronics Engineers Inc. 2023 Jul 31: 111–116.
9. Greitzer FL, Purl J, Leong YM, Becker DES. SOFIT: Sociotechnical and organizational factors for insider threat. In: Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018. Institute of Electrical and Electronics Engineers Inc. 2018: 197–206.
10. Cheng L, Liu F, Yao D. Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2017 Sep;7(5):e1211.
11. Okereafor K, Adelaiye O. Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. International Journal of Recent Engineering Research and Development (IJRERD). 2020;05:61–72.
12. Abdullah F, Salwa Mohamad N, Yunos Z, Malaysia C, Kembangan S. Safeguarding Malaysia's Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. Journal of Cyber Security. 2018;1:22–31.
13. Costa DL, Collins ML, Perl SJ, Albrethsen MJ, Silowash GJ, Spooner DL. An Ontology for Insider Threat Indicators. In: Proceedings of the Ninth Conference on Semantic Technologies for Intelligence, Defense, and Security. 2014: 48–53.
14. Costa DL, Albrethsen MJ, Collins ML, Perl SJ, Silowash GJ, Spooner DL. An Insider Threat Indicator Ontology. Technical Report CMU/SEI-2016-TR-007. 2016 May.
15. Elmrabit N, Yang SH, Yang L, Zhou H. Insider threat risk prediction based on Bayesian network. Comput Secur. 2020 Sep 1;96:101908.
16. Zeng M, Dian C, Wei Y. Risk assessment of insider threats based on IHFACS-BN. Sustainability. 2022 Dec 28;15(1):491.
17. Common Sense Guide to Mitigating Insider Threats,Technical Report.Software Engineering Institute.Seventh Edition. 2022 Sep7. Available from: https://insights.sei.cmu.edu/library/common-

sense-guide-to-mitigating-insider-threats-seventh-edition/
18. Marina Wan Ismail W, Awang Z, Idris I. Exploring and Developing Items Measuring Quality of Life among Heart Failure Patients in Malaysia. Malaysian Journal of Public Health Medicine. 2022;22(1):48–55.
19. Elangovan N, Sundaravel E. Method of preparing a document for survey instrument validation by experts. MethodsX. 2021 Jan 1;8:101326.
20. Hair Jr. JF, Gabriel MLD da S, Patel VK. AMOS covariance-based structural equation modeling (CB-SEM) guidelines on its application as a marketing research tool. Revista Brasileira de Marketing. 2014 May 23;13(2):44–55.
21. Roebianto A, Savitri SI, Aulia I, Suciyana A, Mubarokah L. Content validity: Definition and procedure of content validation in psychological research. TPM - Testing. 2023 Mar 1;30(1):15–18.
22. Heale R, Twycross A. Validity and reliability in quantitative studies. Evid Based Nurs. 2015;18(3):66–67.
23. Nik Mohamed NN, Sahid S, Mahmud MI, Azman N. Exploratory Factor Analysis (EFA) and Reliability Analysis of Financial Well-being Instrument Among Trainee Teachers. International Journal of Academic Research in Accounting Finance and Management Sciences. 2023 Sep;12(3):487-500.
24. Perla RJ, Provost LP. Judgment sampling: A health care improvement perspective. Quality Management in Health Care. 2012; 21: 169–175.
25. Rahlin NA, Awang Z, Fauzi SN. A Mediation Model of Safety Performance in Small and Medium Enterprises: A Structural Equation Modelling. InInternational Conference on Business and Technology 2022 Mar 23 (pp. 856-866). Cham: Springer International Publishing.
26. Ehido A, Awang Z, Abdul Halim B, Ibeabuchi C. Developing Items for Measuring Quality of Work Life Among Malaysian Academics: An Exploratory Factor Analysis Procedure. Humanities & Social Sciences Reviews. 2020 Jun 29;8(3):1295–1309.
27. Fitriana N, Hutagalung FD, Awang Z, Zaid SM. Happiness at work: A cross-cultural validation of happiness at work scale. PLoS One. 2022 Jan 5;17(1):e0261617.
28. Anuar N, Muhammad AM, Awang Z. Development and Validation of Critical Reading Intention Scale (CRIS) for University Students using Exploratory and Confirmatory Factor Analysis. Asian Journal of University Education. 2023;19(1):39–52.
29. Shams A, Hoque MM, Siddiqui A, Awang Z Bin, Awaluddin SM, Baharu T. Exploratory factor analysis of Entrepreneurial orientation in the context of Bangladeshi small and medium Enterprises (SMEs). European Journal of Management and Marketing Studies. 2018 Jun 19;3(2):81-94.
30. Dani RM, Mansor N, Awang Z, Afthanorhan A. A Confirmatory Factor Analysis of the Fraud Pentagon Instruments for Measurement of Fraud in the Context of Asset Misappropriation in Malaysia. Journal of Social Economics Research. 2022 Jul 13;9(2):70–79.
31. Hertzog MA. Considerations in determining sample size for pilot studies. Research in Nursing and Health. 2008 Apr;31(2):180–191.
32. Baharum H, Ismail A, Awang Z, McKenna L, Ibrahim R, Mohamed Z, et al. Validating an instrument for measuring newly graduated nurses' adaptation. International journal of environmental research and public health. 2023 Feb 6;20(4):2860.
33. Nasir MNM, Mohamad M, Ghani NIA, Afthanorhan A. Testing mediation roles of place attachment and tourist satisfaction on destination attractiveness and destination loyalty relationship using phantom approach. Management Science Letters. 2020;10(2):443–454.
34. Shkeer AS, Awang Z. Exploring the Items for Measuring the Marketing Information System Construct: An Exploratory Factor Analysis. International Review of Management and Marketing. 2019 Oct 11;9(6):87–97.
35. Abdol Jani WNF, Razali F, Ismail N, Ismawi N. Exploratory factor analysis: Validity and reliability of teacher's knowledge construct instrument. International Journal of Academic Research in Progressive Education and Development. 2023 Jan;12(1):944–953.
36. Tavakol M, Dennick R. Making Sense of Cronbach's Alpha. Int J Med Educ. 2011 Jun 27; 2:53–55.
37. Taber KS. The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. Res Sci Educ. 2018 Dec 1;48(6):1273–1296.
38. Dehisat MM, Awang Z. Exploring Items and Developing Instrument for Measuring Organizational Performance among Small Medium Enterprises in Jordan. International Review of Management and Marketing. 2020 Nov 5;10(6):51–57.
39. Bahkia AS, Awang Z, Afthanorhan A, Ghazali PL, Foziah H. Exploratory factor analysis on occupational stress in context of Malaysian sewerage operations. In AIP Conference Proceedings. AIP Publishing. 2019 Aug 21; 2138(1):050006.