REVEALING THE MULTI-PERSPECTIVE FACTORS BEHIND INSIDER THREATS IN CYBERSECURITY

Nur Fahimah Mohd Nassir, Ummul Fahri Abdul Rauf*, Zuraini Zainol, Kamaruddin Abdul Ghani
Universiti Pertahanan Nasional Malaysia
ummul@upnm.edu.my

Received Date: 28/6/2024 *Accepted Date: 9/9/2024* *Published Date:30/10/2024*

Abstract

In the realm of cybersecurity, insider threats persist as significant challenges for organisations globally. Despite increasing acknowledgement of their impact, there is a lack of comprehensive studies that explore the multi-perspective factors contributing to insider threat occurrence from a holistic standpoint. This study aims to address this gap by conducting a thorough analysis of the human, technical, and organisational elements influencing insider threats. Through a content analysis approach, this study delves into the intricate interplay of individual characteristics, technical vulnerabilities, and organisational practices that can give rise to insider threats. This methodology involves systematically collecting, coding, and analysing a diverse range of textual data sources to identify recurring themes and patterns related to insider threats. We employed the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) method to systematically review the literature. We conducted a literature search on Scopus, Web of Science, and IEEE for articles published between 2014 and 2023. We discovered a total of thirty-two (32) articles that were relevant for further analysis. The data indicates that human factors consist of five themes and fifteen sub-themes, technical factors have one theme and four sub-themes, and organisational factors have four themes and fifteen sub-themes. Overall, this study emphasises the importance of approaching insider threats from multiple perspectives, since no single factor operates independently. Instead, it is the combination and interaction of human, technical, and organisational components that create vulnerabilities and opportunities for insider threats.

Keywords: *Content analysis, cyberthreat, insider threat, PRISMA.*

1.0 Introduction

The rapid growth of information technology revolution such as emergence of artificial intelligence (AI), internet of things (IoT), and big data in recent years has resulted in numerous advancements that have revolutionized how individuals, business, and government interact, communicate, and operate on a global scale [1]. However, this progress has also ushered in new challenges, particularly in the realm of cybersecurity. As technology continues to evolve, so do the methods and tactics of cyberthreat and attacks, posing significant risks to individuals, organisations, and even entire economies.

Within the broader spectrum of cyberthreat, insider threats have emerged as a significant and insidious concern. Unlike external threats, insider threats are originated from individuals within the organisation, including employees, contractors, or business partners, who have legitimate access to assets such as sensitive information and system, exploit their access rights to cause harm or disclose sensitive information [2]. Insider threats can stem from various factors, including human behaviours, technical vulnerabilities, and organisational shortcomings [3]. Based on [4], these threats can have disastrous consequences, resulting in significant financial losses and reputational damage. In addition, insider attacks can compromise the confidentiality, integrity, and availability of sensitive data, leading to serious consequences such as data

leakages, intellectual property theft, and industrial espionage [5].

As stated in [6], insider threats are influenced by a combination of behavioural, technical, and organisational factors. It is worth noting that researchers have conducted extensive studies and developed frameworks to enhance understanding and mitigation strategies [7]. Between 2014 and 2023, multiple ontologies and frameworks were developed to address cybersecurity and insider threats. These ontologies differ in their application domains, scopes, representation formalisms, and types of constructs represented.

It is worth noting that early studies from 2014 and 2015 focused on creating frameworks based mainly on technical indicators such as Insider Threat Indicator Ontology (ITIO) activity [8], Structured Threat Information Expression (STIX) [9], and Human Factors Ontology (HUFO) [10]. Among these, ITIO was specifically designed to detect both behavioral and technical indicators of malicious insider activity. These indicators include unusual behavior patterns, access logs, data exfiltration attempts, policy violations, and other suspicious activities. The ontology primarily relies on resources such as the compilation of insider threat cases from the Multiple East-West Railways Integrated Timetable Storage (MERIT) database.

In 2018, Greitzer et al. [11] designed and developed a structured model that emphasizes individual and organisational sociotechnical factors, integrating technical indicators from previous work. This study recommended adding an additional construct to the ontology to further specify the lower-level leaf nodes.

Additionally, in 2020, Elmrabit et al. [3] began integrating human factors with technical and organisational aspects. This study introduced an insider threat risk prediction framework that employs multi-perspective concepts to anticipate malicious insider threats before a breach occurs. This framework, however, focuses solely on factors that contribute to malicious insider threats. On the other hand, the epidemiological triangle in [12] represents the interplay between three vectors of exploit, user, and work environment that tackle intentional and unintentional insider threats. Nevertheless, this study mainly focuses on unintentional insider threats and offers a series of recommendations to mitigate their negative impacts.

More recently, Zeng et al. [13] proposed an improved Human Factors Analysis and Classification System (IHFACS) based on actual enterprise management to enhance insider threat risk assessment. This study emphasised the importance of exploring key human factors to effectively prevent insider threats. Figure 1 illustrates a summary and comparison of ontology and framework representations for cybersecurity and insider threat domains.

Ontology/ Framework	Domain/Scope	Year	Human/ Behaviour	Technical	Organisational
Insider Threat Indicator Ontology (ITIO)	Insider Threat	2014	✓	✓	
Structured Threat Information Expression (STIX)	Cybersecurity	2014		✓	
Human Factors Ontology (HUFO)	Cybersecurity - Trust	2015	✓	✓	
Sociotechnical and Organizational Factors for Insider Threat (SOFIT)	Insider Threat	2018	✓		✓
Insider Threat Risk Prediction	Insider Threat – Malicious	2020	✓	✓	✓
Epidemiological Triangle	Insider Threat – Unintentional	2022			✓
Human Factors Analysis and Classification System (IHFACS)	Insider Threat	2023	✓		✓

Figure 1. Ontology and Framework in Cybersecurity and Insider Threat

Due to the aforementioned scenarios, it is evident that while there is a growing amount of study on insider threats, there is still s a gap in addressing the issue from multiple perspectives, encompassing both

malicious and unintentional insiders. Motivated by this identified gap in the literature, this study will conduct a thorough analysis to explore the human, technical, and organisational factors that contribute to insider threats, using content analysis based on previously documented studies. Through this endeavor, we aspire to contribute valuable insights into the fundamental elements required to address this issue.

2.0 Methodology

The study implemented a qualitative research design that integrates two complementary methodologies to conduct a thorough investigation of insider threats. Qualitative research is a procedure that aims to comprehend phenomena in depth by focusing on subjective experiences, meanings, and perspectives [14]. It involves collecting and analysing non-numerical data to gain insights into complex issues or explore new areas of study [15].

The first approach involved conducting a systematic literature review (SLR), following the guidelines of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). This method ensured a rigorous and transparent process for identifying, selecting, and synthesising relevant studies, providing a solid foundation for the subsequent analysis [16]. We methodically conducted the SLR process in several key steps to ensure a comprehensive and rigorous examination of the existing literature. The process began with the establishment of eligibility criteria, where specific inclusion and exclusion parameters were defined. We then implemented a detailed search strategy, utilising three major databases: Scopus, Web of Science (WoS), and Institute of Electrical and Electronics Engineers (IEEE). Next, we initiated the study selection process by screening the titles and abstracts of the retrieved articles. We then conducted a thorough review of the full-text articles that met the preliminary screening criteria, ensuring they aligned with the predefined eligibility criteria. Finally, we conducted the data extraction phase, systematically collecting and analysing key information from the selected studies.

Content analysis, a qualitative method, served as the second approach, systematically examining and interpreting the content of various forms of communication, such as texts, images, and audio or video materials [17]. Moreover, content analysis is particularly well-suited for examining patterns, themes, and meanings within textual data, allowing researchers to uncover underlying factors and relationships that may not be immediately apparent [18]. This study employed content analysis to identify and explore key themes related to human, technical, and organisational factors influencing insider threats. The process included coding the data, clustering similar codes into categories, and then grouping these categories into broader themes. Overall, this method provided valuable insights and a nuanced understanding of the factors that contribute to insider threats.

2.1 Eligibility Criteria

The eligibility criteria for documented studies in a systematic review perform several essential functions that are critical for producing a valid and reliable synthesis of the available evidence. These criteria define the scope of the review, ensuring that the included studies are relevant to the research question and of high quality. By reducing heterogeneity among the selected studies, the criteria help maintain the synthesis's coherence and comparability. Moreover, the eligibility criteria guide the screening process, providing clear guidelines for reviewers to determine which studies to include or exclude [19]. This approach ensures a consistent and transparent method of study selection, which is essential for producing a robust and trustworthy synthesis of the available evidence. To choose which publications to include or exclude in our study, we applied the specific eligibility criteria outlined in Table 1.

TABLE 1
Criteria of the Inclusion and Exclusion in the Primary Study

Inclusion Criteria	Exclusion Criteria
The paper should focus on factors that contribute to or influence insider threat occurrences.	The research of the paper does not focus to identify or related to insider threat factors.
The paper needs to be published as a research article.	Article published earlier than 2014.
The paper is written in the English language.	The paper does not adequately discuss the findings.

2.2 Search Strategy

A well-designed search strategy increases the retrieval of pertinent studies while limiting irrelevant results, thereby ensuring that the review is comprehensive and unbiased. We selected relevant articles for this study using a search engine-based literature search. Specifically, the literature search focused on articles or journals related to insider threats published in impact journals, conference articles, and book sections, primarily in online databases such as Scopus, WoS, and IEEE, covering publications from 2014 to 2023. We selected these databases for the literature search because they comprehensively cover high-quality research across various disciplines and have a strong reputation for indexing peer-reviewed research to high standards. Moreover, the decision to focus on publications from 2014 to 2023 was deliberate, as this period captures the most recent and relevant research in the rapidly evolving field of cybersecurity and insider threats [7].

Additionally, we conducted the search using carefully selected keywords and term combinations designed to capture the most relevant studies in this domain. In particular, we used the following keywords for the literature search: "cybersecurity," "insider threat," "human factor," "technical factor," and "organisational factor." The selection of keywords was based on the core concepts and variables under investigation in this study. For instance, we used terms like "cybersecurity" to broaden the field's scope, and specifically targeted the research focus with "insider threat". Furthermore, the inclusion of keywords such as "human factor," "technical factor," and "organisational factor" ensured the inclusion of studies addressing the multifaceted aspects of insider threats. By selecting these terms, the study aimed to reflect the various dimensions of insider threats, particularly the human, technical, and organisational elements that contribute to such risks. Figure 2 shows the search engines for each of the scientific databases that met the search criteria.

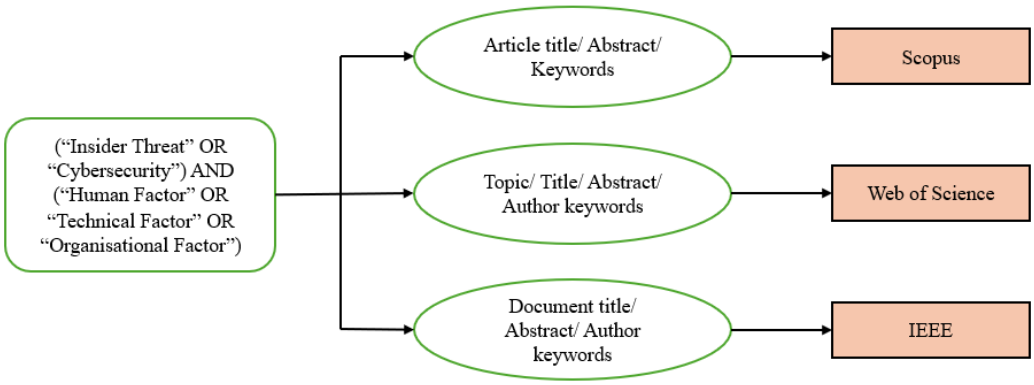

Figure 2. Search Strategy in Multiple Database

2.3 Study Selection

We meticulously screened full-text articles against the eligibility criteria in order to ensure the inclusion of pertinent and high-quality studies. Initially, all retrieved articles underwent a preliminary screening based on their titles and abstracts. This step was intended to quickly eliminate studies that were clearly irrelevant to the research topic, such as those focusing solely on external cyber threats or studies examining technical aspects outside the scope of insider threats.

For the articles that passed the initial screening, we obtained full-text versions and conducted a comprehensive review. We carried out a detailed assessment against the predefined eligibility criteria during this stage, which included publication dates ranging from 2014 to 2023, the type of publication (peer-reviewed journal articles, conference papers, technical papers, and reputable white papers), and a focus on insider threats from human, technical, or organisational perspectives.

The final synthesis included only studies that met all predefined eligibility criteria. As a result, these selected studies provided relevant insights and empirical data critical for understanding insider cyber threats. Additionally, for studies that did not meet the eligibility criteria, we systematically documented the specific reasons for exclusion.

2.4 Data Extraction

During the data extraction process, we meticulously gathered relevant information from the full-text articles that met the predefined eligibility criteria. Specifically, we extracted data on the study's objectives and key findings, focusing on human, technical, and organizational factors related to insider threats. To ensure uniformity and reliability across all included studies, we used a standardised data extraction form. We simultaneously screened and excluded full-text articles according to the following criteria:

- Unavailability of full-text: Articles were excluded due to the unavailability of full-text versions, despite comprehensive searches through databases and other sources.
- Unpublished articles: To maintain high quality and reliability, unpublished articles were excluded.
- Mismatch with inclusion criteria: If a full-text article was found to not meet the predefined inclusion criteria upon review, it was excluded from further analysis.
- Inappropriate findings or discussion: Articles were excluded if their findings or discussions were not in line with the objectives and scope of our study.

2.5 Content Analysis

The content analysis began with the development of a coding scheme, which served as the foundational framework for categorising and interpreting the data. We developed this coding scheme based on a preliminary review of the literature and the study's specific research objectives. It included predefined codes representing key aspects of insider threats, such as motivations and behaviours of insiders, technical vulnerabilities, organisational practices, and proposed frameworks or ontologies. Each code was clearly defined to ensure consistency and clarity in the coding process.

During the coding process, we opted to use Microsoft Excel manually. We chose this approach to maintain close engagement with the data, enabling a deeper understanding and more nuanced interpretation of the findings. By manually listing all the factors contributing to insider threat risk, as mentioned in previous studies, we were able to systematically categorise these factors into three main categories: human, technical, and organizational. This hands-on approach also provided the flexibility to refine codes and categories as the analysis progressed, ensuring that the coding remained closely aligned with the research objectives.

We systematically coded the content of the selected articles once we established the coding scheme. This process involved reading each article thoroughly and assigning relevant codes to specific segments of text that addressed the research objective. We then clustered the coded data into broader categories based on thematic similarities. For instance, we grouped codes related to insider motivations and behaviours together, while categorising codes related to technical weaknesses and organisational shortcomings separately. Following the coding and categorisation, we further analysed the categorised data to discover overarching themes and patterns.

3.0 Result

The systematic review process began with the comprehensive search of the selected platform's database, with the identification of a total of 494 studies. We obtained the papers from three main databases: Scopus (238 articles), Web of Sciences (158 articles), and IEEE (98 articles). After eliminating duplicate studies, we reduced the number to 128. Following this, we carried out a comprehensive evaluation procedure known as title and abstract screening, applying eligibility criteria to either include or exclude search results. Subsequently, we thoroughly assessed the research that met the specific criteria for inclusion and exclusion, resulting in a total of 67 publications for further study. A rigorous assessment and data extraction process resulted in the elimination of 35 more articles. Ultimately, we selected a total of 32 studies for further study, fulfilling all the predetermined criteria. Figure 3 illustrates our implementation of the PRISMA methods adapted from [20], which consist of four primary phases: identification, screening, eligibility, and inclusion, for the purpose of selecting the relevant publications.

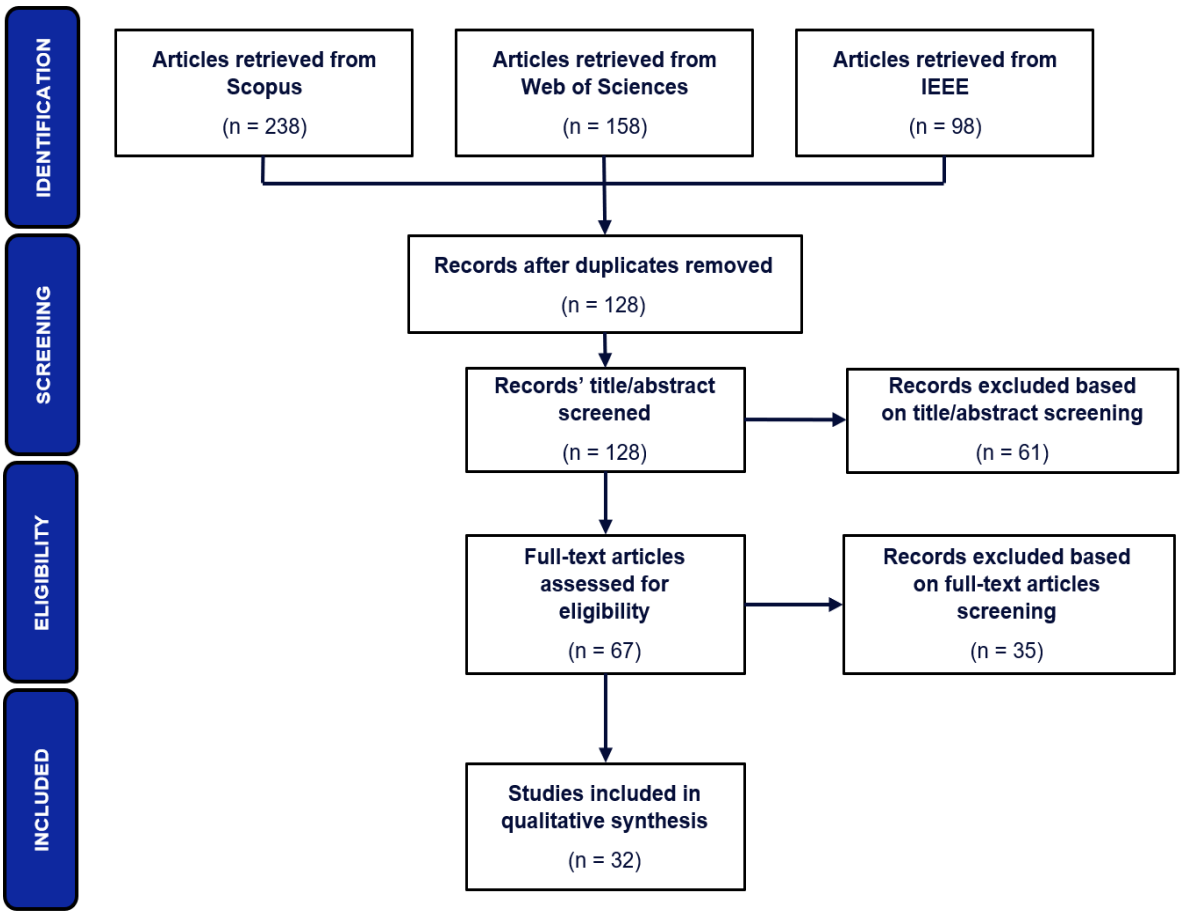

Figure 3. PRISMA Flow Diagram (adapted from Moher et. al [20])

The content analysis identified eleven major themes that influence insider threats, categorising them into human, technical, and organisational factors. For human factors, the themes identified were inadequate security training and awareness, mental health issues, personal problems, and negative personality traits. These themes reflect the critical role that human vulnerabilities play in contributing to insider threats. In terms of technical factors, the identified themes were a lack of resources, inadequate monitoring systems, and weak security evaluation and validation. These themes highlight gaps in technological infrastructure and oversight that make organisations susceptible to insider threats. Lastly, for organisational factors, the themes included issues with organisational practices, insufficient risk management, poor management systems, and workplace stressors. In order to enhance the reader's understanding of the study's findings, we break down the results into subheadings in each analysis.

3.1 Human Factor

The analysis of human factors revealed four main themes, each of which contained a total of 15 sub-themes. The first theme, Inadequate Security Training and Awareness, emerged from code keywords like "awareness or knowledge" and "training." We grouped these keywords into the sub-categories of Lack of Information Security Knowledge and Insufficient Training on Security Policies. These sub-categories highlight how inadequate security training and awareness among employees may be significant factors

contributing to the occurrence of insider threats.

The second theme, Mental Health Issues, encompasses sub-subjects such as deep frustration and stress, both of which may lead individuals to engage in insider threat activities. We derived these sub-themes from code keywords like "frustration" and "stress."

Next, Personal Problems emerged as the third theme, encompassing keywords like "financial," "divorce," "addiction or substance abuse," "coercion or blackmail," and "disgruntlement or dissatisfaction." These keywords led to the formation of the sub-categories Financial Issues, Relationship Conflict, Addiction or Substance Abuse, Blackmail, and Disgruntlement or Dissatisfaction with the Organisation or Job. Personal issues like these can have a significant influence on insider behaviour.

Finally, we derived the fourth theme, Negative Personality Traits, from keywords such as "curiosity," "communication," "carelessness, negligence, or recklessness," "resistance," "mischievousness," "loyalty," and "greed." These codes were grouped into sub-themes including Curiosity, Poor Interpersonal Relationships, Carelessness or Negligence, Resistance, Mischievousness, Disloyalty Towards the Organisation, and Greed. These specific personality traits heighten the likelihood of insider threats by driving individuals to engage in risky or malicious actions.

Table 2 illustrates the detailed coding and categorization of these themes and sub-themes.

TABLE 2
Human Factors that Influence Insider Threat

Authors/ Citation	Code/ Keyword	Sub-theme/ Category	Theme	Example Quote/ Description
[13], [21], [22], [23], [24], [25], [26], [27]	Awareness/ Knowledge	Lack of awareness on information security	Inadequate security training & awareness	“A lack of awareness, negligence, resistance, disobedience, apathy and mischievousness are root causes of information security incidents in organisations.”
[23], [24], [28], [29], [30], [31], [32], [27]	Training	Insufficient training on security policies and procedures		“...previous incidents might well have highlighted the employee’s lack of training or need for supervision, or it might have served to highlight flaws in the day-to-day procedures when transferring sensitive data.”
[23], [25], [33]	Frust	Deep frustration	Mental health issues	“Personal factors, which include introversion, handling stress and deep frustration are the common factors for identifying insider attacks.”
[13], [22], [34], [33], [25], [30], [35]	Stress	Stress		“Employees can make mistakes due to “fatigue”, “stress”, “overwork”, “inattention”, or “multitasking”…”

[22], [36], [33], [37], [38], [39], [23], [40], [41]	Financial	Financial issue	Personal problems	"...family, financial issues, health issues, all of these factors influence the employee to perform threats like blackmail or stealing information for monetary benefit."
[38], [39], [30]	Divorce	Relationship conflict		"…psychosocial factors—like a stressful divorce, difficulty working with others, or retaliatory behavior—may affect the insider threat."
[37], [39], [40], [27]	Addiction/ Substance abuse	Addiction or substance abuse		"…from a malicious, insider-threat perspective, examples of notable behaviours include addictive practices (e.g., gambling or alcohol abuse), previous rule violations…"
[22], [33], [42]	Coercion/ Blackmail	Blackmail		"…blackmailing insiders are other tactics."
[43], [22], [23], [44], [11], [41], [45]	Disgruntlement/ Dissatisfaction	Disgruntlement/ dissatisfaction with the organisation or job		"…resulted in disgruntlement and behaviors—e.g., violations of policies, rules, or even laws—that could have provided warning of increased insider risk."
[34], [23], [11]	Curiosity	Curiosity	Negative personality traits	"…caused by the intentional misuse of privileges without an intention to cause harm, such as using their privileges to access confidential information of a celebrity client out of curiosity."
[13], [24], [33], [11]	Communication	Poor interpersonal relationship		"…the generic cause for the clash between the organization like RMP and employee was due to limited communication, misunderstanding or misperception or differences in opinion."
[22], [46], [26], [11], [30]	Careless/ Negligence/ Reckless	Careless/ Negligence		"Unintentional incidents happen due to human nature, such as ignorance, carelessness, stress, or fatigue."
[43], [26], [11]	Resistance	Resistance		"…resistance, disobedience, apathy and mischievousness are root causes of information security incidents in organisations."

[26]	Mischievousness	Mischievousness		"…resistance, disobedience, apathy and mischievousness are root causes of information security incidents in organisations."
[22], [23], [33], [41]	Loyal	Disloyalty towards the organisation		"…a lack of loyalty among young generations and employee mistakes that arise from human nature."
[13], [22], [30]	Greed	Greed		"Most insider threat incidents are the consequences of human actions, such as mistakes, negligence, greed, or reckless behavior."

3.2 Technical Factor

The analysis of technical factors identified three main themes, revealing a total of four sub-themes, all of which highlight critical gaps in technological infrastructure and oversight that contribute to insider threats. First, the theme of Lack of Resources emphasises how deficiencies in organisational resources create vulnerabilities in defence mechanisms, which can lead to the emergence of insider threats. We derived this theme from keywords such as "hardware," "software," "network," and "infrastructure," and grouped them into the sub-category Poor Information Technology Infrastructure, reflecting how inadequate technological resources undermine security frameworks.

Second, the theme of Inadequate Monitoring Systems underscores the inability of organisations to effectively monitor insider activities in real-time, which significantly increases the risk of undetected insider threats. The keyword "technical monitoring" inspired the sub-theme Weak Technical Monitoring. Thus, the absence of robust monitoring systems may become a critical weakness in mitigating insider threats.

Lastly, the third theme, Weak Security Evaluation and Validation, points to the lack of thorough testing and validation of security systems and applications, particularly in the context of insider threats. Keywords such as "testing" and "assessment" led to the formation of two sub-categories: Insufficient Security Testing and Evaluation of Systems and Applications and Inadequate Insider Threat Vulnerability Assessments. These sub-categories reflect how inadequate evaluation processes leave organisations exposed to internal vulnerabilities that could be exploited by insiders.

The detailed technical factor coding and categorisation of these themes and sub-themes, along with relevant quotations from the literature, are presented in Table 3.

TABLE 3
Technical Factors that Influence Insider Threat

Authors/ Citation	Code/ Keyword	Sub-theme/ Category	Theme	Example Quote/ Description
[22], [11], [27]	Hardware/ Software/ Network/ Infrastructure	Poor information technology infrastructure	Lack of Resources	"The information-technology (IT) factor applies to poorly developed infrastructure and involves the issues of hardware and software information security."

[13], [37], [25]	Technical Monitoring	Weak technical monitoring	Inadequate Monitoring System	"…The factors were named as (1) Technical monitoring and detection, (2) Technical restrictions, and (3) Technical access."
[37]	Testing	Insufficient security testing and evaluation of systems and applications	Weak Security Evaluation & Validation	Penetration testing is one of the factor items for the Organisational Vulnerability to Intentional Insider Threat (OVIT)-Technical.
[43], [37], [44], [31]	Assessment	Inadequate insider threats vulnerability assessments		"Conducting insider threats vulnerability assessment is also a good security strategy to protect organizations against malicious insiders…"

3.3 Organisational Factor

The analysis of organisational factors revealed four key themes: Organisational Practice Issues, Insufficient Risk Management, Poor Management Systems, and Workplace Stressors. Collectively, these themes highlight the critical role that organisational structures and environments play in contributing to insider threats.

Firstly, Organisational Practice Issues underscores the importance of organisational culture in shaping security outcomes. Within this theme, five sub-themes emerged: Poor Organisational Culture (Human Resources (HR) practices), Lack of Security Culture, Level of Trust Issue, Poor Employee's Communication and Collaboration, and Lack of Access Control. These sub-themes were derived from keywords like "organisational culture," "security," "trust," "communication," and "access control." Together, they illustrate how disjointed internal practices create vulnerabilities that insiders can exploit.

Secondly, Insufficient Risk Management reflects gaps in organisations' ability to anticipate and respond to potential threats. This theme was drawn from keywords such as "incident response" and "risk management." The sub-themes identified include the Lack of Proper Incident Response Planning and Inadequate Risk Assessments. These shortcomings reveal how organisations fail to put effective safeguards in place, leaving them exposed to insider risks.

Next, Poor Management Systems as the third theme, points to weaknesses in leadership and operational structures. Here, five sub-themes emerged: Poor Hiring Processes, Insufficient Behavior Monitoring Mechanisms, Lack of Security Policies and Procedures, Information Sharing Process Weaknesses, and Inadequate Security Training and Awareness Programmes. These sub-themes were clustered from keywords like "employment," "monitoring," "policy," "information sharing," and "training." This theme highlights how leadership failures and policy gaps allow security vulnerabilities to flourish within the organisation.

Lastly, Workplace Stressors, the fourth theme, focusses on the impact of environmental stress on insider threats. The sub-themes include High Workload, Stressful Work Environment, and Unfair Work Setting. Keywords like "workload," "stress environment," and "unfair work" were grouped to reflect these conditions. These factors often push employees towards behaviours that may compromise organisational security.

Table 4 provides a detailed breakdown of the coding and categorisation of these themes and sub-themes, supported by relevant quotations from the literature.

TABLE 4
Organisational Factors that Influence Insider Threat

Authors/ Citation	Code/ Keyword	Sub-theme/ Category	Theme	Example Quote/ Description
[13], [12], [47], [37], [40]	Organisational culture	Poor organisational culture (HR practices)	Organisational Practices Issues	"Such a culture may cause employees to disregard the processes, thus increasing the chances of an insider attack succeeding."
[13], [21], [37], [25]	Security	Lack of security culture		"…many organizations consider the knowledge and skills of an employee during job hiring process and give less concern about background of employee related to ICT security concerns."
[13], [34], [23], [33]	Trust	Level of trust issues		"An employee who is trusted will have the potential to cause more harm to the organization by collapsing the stability of the computing systems."
[11], [40], [41]	Poor communication	Poor employee's communication & collaboration		"Workplace conditions that foster human errors or deficiencies in human performance may be described in terms of a variety of issues, including poor communications relating to a task and its goals, confusing procedures, faulty system design that reduces usability."
[13], [22], [21], [43], [25],	Access/ Security control	Lack of access control		"Another factor driving insider cybersecurity threats is the lack of oversight of staff access to technology."
[12]	Incident response	Lack of incident response planning	Insufficient Risk Management	"Speed of the incident, discovery and response is one of the task factors items."
[13], [22], [11]	Risk management	Inadequate risk assessment		"Cognitive biases are factors that contribute to human error, poor judgment, and flawed risk assessments that potentially increase the likelihood of UIT incidents."

[13], [29] [11], [41]	Employment	Poor hiring process	Poor Management System	"Failure to conduct pre-employment background checks on employees or pre-job reviews of confidential personnel is mere formalities."
[37], [38], [29], [11]	Monitoring	Inadequate behaviour monitoring mechanism		An employer, for example, might notice an employee who presents a problematic behaviour and provide them with support or closer monitoring to assist in prevention and detection.
[13], [22], [38], [37], [25], [11], [41]	Policy/ Procedure	Lack of security policies and procedures		"Prevention, therefore, might involve strengthening security and the development of workplace policy to close down on insider threat opportunities…"
[25]	Sharing information	Information sharing process weaknesses		"In some cases, surprisingly some working colleagues still sharing credentials among themselves to execute daily tasks, in which a malicious insider would take advantage to misuse the opportunity."
[13], [29], [11], [41]	Training employees	Inadequate security training and awareness programmes		Training the employees in the organization and developing an information security culture are great boons in implementing proper security measures inside the organizations.
[12], [11], [41], [32]	Workload	High workload	Workplace Stressor	"Organisational factors refer to management practices, policies, work environment, workload, and related aspects of the workplace that may contribute to performance deficiencies and human error, which play a significant role in the unintentional insider threat."
[22], [12], [36], [38], [25]	Stress environment	Stressful work environment		Working environment that does not follow standard, and recognition could distract insiders.

[25], [41]	Unfair work	Unfair work setting		"...employees need to be free from external distractions such as pressures from superiors, unrealistic work schedule, insufficient remunerations and uneven job separations."

4.0 Discussion

This paper, unlike previous studies, adopts a broader perspective, considering the multi-perspective factors of both malicious and unintentional insiders that influence insider threat occurrences. In a previous study, Elmrabit et al. [3] mentioned in their developed framework that there are three human factors that allow malicious insiders to misuse their privileges. These include motivation, opportunity, and capability. However, our findings revealed four themes related to human factors that are prone to unintentional and malicious cyber insider threat actions. This study emphasises the need for organisations to enhance awareness about information security risks [21] and ensure that employees receive adequate training on security policies and procedures [28] to mitigate the risk of insider threats stemming from a lack of knowledge or understanding. Furthermore, [33] stress the vulnerabilities in mental health are the most common indicator of a potential insider attack. To address this issue, mental health scanning and monitoring programs are required. In the meantime, experts underscored the importance of tackling personal issues such as financial difficulties [39], relationship conflicts [38], substance abuse [40], blackmailed [42], and dissatisfaction with the organisation or job [13] decrease instances of insider threats.

In terms of technical factors, compared to existing literature, we found three main themes. A lack of resources, such as hardware, software, networks, and other information technology infrastructure [22], as seen in the first theme, highlights issues related to poor information technology infrastructure. This deficiency is critical because it creates opportunities for insider threats to exploit system vulnerabilities. Additionally, there are insufficient systems for monitoring insider activities, making it challenging to detect malicious actions in real-time [13]. Robust monitoring systems are essential for identifying potential threats promptly and mitigating risks before significant damage occurs [25]. For identifying and addressing security gaps that insider threats could exploit, effective penetration testing and comprehensive vulnerability assessments are crucial [37]. Organisations must prioritise investment in robust technical systems and continuous evaluation to stay ahead of potential insider threats.

Regarding the organisational factors, identified themes highlight systemic vulnerabilities that contribute to both malicious and unintentional insider threats. The analysis in this study revealed significant implications for organisational security practices. The identification of organisational practice issues such as poor organisational culture [12], lack of security culture [21], high level of trust with our colleagues [34], weak communication and collaboration between the departments [11], and poor access control [22] underscores the need for a holistic approach to enhancing internal processes. Similarly, the deficiencies in incident response planning and risk assessments [12] point to the necessity for robust risk management strategies. Furthermore, the inadequacies in management systems, such as ineffective hiring practices [13] and monitoring behaviour mechanisms [38], further exacerbate the risk by failing to identify potential insider threats early. Lack of security policies and procedures [41], poor information sharing practices [25], and insufficient security training and programmes organised by the organisation [29] also emerged as critical vulnerabilities. Allocating adequate budgets to address these deficiencies is crucial. Organisations need to invest in developing and implementing comprehensive security policies, enhancing information sharing mechanisms, and providing regular, thorough training programmes to ensure all employees are well-versed in security protocols. Moreover, high workload [32], high-stress environment [22], and unfair work conditions [25] indicate the importance of creating a supportive and equitable work environment in

order to mitigate insider threat incidents.

While this study offers valuable insights into insider threats, it is important to acknowledge certain limitations inherent in the PRISMA and systematic literature review (SLR) methodologies. One key limitation, however, is the tendency to rely heavily on high-impact and well-established journals, which may inadvertently exclude valuable insights from newer or region-specific publications. Although these less prominent sources are not as widely recognised, they may contain context-specific information crucial for understanding insider threats in particular regions or industries. As a result, this limitation means that the analysis may not fully capture the diversity of insider threat issues present in different geographic and cultural contexts.

In order to build on the findings of this study, future research should not only expand the literature review to include more diverse sources but also incorporate interviews or focus group discussions with cybersecurity experts and practitioners. Interviews with subject matter experts (SMEs) have the potential to reveal practical insights and experiences that academic publications often fail to capture. Thus, this approach would provide a more holistic view of how insider threats are managed across different industries and regions.

Moreover, it may be beneficial for future studies to explore the role of emerging technologies, such as artificial intelligence (AI) and machine learning (ML), in enhancing the detection and prevention of insider threats. As these technologies advance, they have the potential to significantly improve the monitoring of insider activities and the identification of suspicious behavior patterns. Therefore, investigating the integration of these technologies into current security frameworks could yield significant advancements in the field.

5.0 Conclusion

This study has provided a comprehensive analysis of the human, technical, and organisational factors that influence the occurrence of both malicious and unintentional insider threats. We have identified significant vulnerabilities within organisations that require attention to improve their cybersecurity posture. The identified human factors, including inadequate security training, mental health issues, personal problems, and negative personality traits, underscore the importance of focusing on the human element in cybersecurity strategies. Technical factors, such as poor IT infrastructure, inadequate monitoring systems, and weak security evaluation and validation, reveal the need for robust technical defences and continuous assessment of security measures. Meanwhile, organisational factors such as organisational practice issues, insufficient risk management, poor management systems, and workplace stressors point to systemic issues requiring strategic changes.

In light of this, it is recommended that future studies employ a survey questionnaire tailored to the specific context of insider threats. Such a survey could facilitate a more nuanced exploration of human, technical, and organisational factors, as well as the collection of quantitative data that complements the qualitative insights provided by this study. By using a survey, researchers can capture a wider range of perspectives and experiences, enriching their overall understanding of insider threat occurrences.

6.0 References

[1] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review,” *J Big Data*, vol. 6, no. 1, Dec. 2019, doi: 10.1186/s40537-019-0268-2.

[2] J. Hunker, A. Llc, and C. W. Probst, “Insiders and Insider Threats An Overview of Definitions and Mitigation Techniques.”

[3] N. Elmrabit, S. H. Yang, L. Yang, and H. Zhou, "Insider Threat Risk Prediction based on Bayesian Network," *Comput Secur*, vol. 96, Sep. 2020, doi: 10.1016/j.cose.2020.101908.
[4] K. Kisenasamy, S. Perumal, V. Raman, and B. S. M. Singh, "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*, vol. 13, pp. 236–251, Mar. 2022, doi: 10.1007/s13198-021-01378-3.
[5] Z. M. Yusop and J. H. Abawajy, "Analysis of Insiders Attack Mitigation Strategies," *Procedia Soc Behav Sci*, vol. 129, pp. 611–618, May 2014, doi: 10.1016/j.sbspro.2014.06.002.
[6] "Common Sense Guide to Mitigating Insider Threats 7th Edition," 2022.
[7] N. F. M. Nassir, U. F. A. Rauf, Z. Zainol, and K. A. Ghani, "Insider Threat Prediction Techniques: A Systematic Review," in *Tech Horizons: Unveiling Future Technologies*, 2024, pp. 119–126.
[8] D. L. Costa, M. L. Collins, S. J. Perl, M. J. Albrethsen, G. J. Silowash, and D. L. Spooner, "An Ontology for Insider Threat Indicators Development and Applications," pp. 48–53, Nov. 2014.
[9] "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)," 2012. [Online]. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pd
[10] D. S. Henshel, M. G. Cains, B. Hoffman, A. Oltramari, D. Henshel, and M. Cains, "Towards a Human Factors Ontology for Cyber Security," *Semantic Technologies for Intelligence, Defense, and Security*, 2015.
[11] F. L. Greitzer, J. Purl, Y. M. Leong, and D. E. S. Becker, "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., Aug. 2018, pp. 197–206. doi: 10.1109/SPW.2018.00035.
[12] N. Khan, R. J. Houghton, and S. Sharples, "Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks," *Cognition, Technology and Work*, vol. 24, no. 3, pp. 393–421, Aug. 2022, doi: 10.1007/s10111-021-00690-z.
[13] M. Zeng, C. Dian, and Y. Wei, "Risk Assessment of Insider Threats Based on IHFACS-BN," *Sustainability (Switzerland)*, vol. 15, no. 1, Jan. 2023, doi: 10.3390/su15010491.
[14] A. Bazen, F. K. Barg, and J. Takeshita, "Research Techniques Made Simple: An Introduction to Qualitative Research," Feb. 01, 2021, *Elsevier B.V.* doi: 10.1016/j.jid.2020.11.029.
[15] C. N. Ugwu and E. Val, "Qualitative Research," *IDOSR JOURNAL OF COMPUTER AND APPLIED SCIENCES*, vol. 8, no. 1, pp. 20–35, 2023, [Online]. Available: www.idosr.org
[16] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *J Clin Epidemiol*, vol. 134, pp. 178–189, Jun. 2021, doi: 10.1016/j.jclinepi.2021.03.001.
[17] M. Bengtsson, "How to plan and perform a qualitative study using content analysis," *NursingPlus Open*, vol. 2, pp. 8–14, 2016, doi: 10.1016/j.npls.2016.01.001.
[18] H. F. Hsieh and S. E. Shannon, "Three approaches to qualitative content analysis," *Qual Health Res*, vol. 15, no. 9, pp. 1277–1288, Nov. 2005, doi: 10.1177/1049732305276687.
[19] C. Weng, S. W. Tu, I. Sim, and R. Richesson, "Formal representation of eligibility criteria: A literature review," Jun. 2010. doi: 10.1016/j.jbi.2009.12.004.
[20] D. Moher *et al.*, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," Jul. 01, 2009, *Public Library of Science*. doi: 10.1371/journal.pmed.1000097.
[21] M. L. Green and P. Dozier, "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, pp. 111–116. doi: 10.1109/CSR57506.2023.10224926.
[22] A. Á. Mészáros and A. Kelemen-Erdős, "Industrial espionage from a human factor perspective," *Journal of International Studies*, vol. 16, no. 3, pp. 97–116, 2023, doi: 10.14254/2071-8330.2023/16-

3/5.
[23] S. Prabhu and N. Thompson, "A Unified Classification Model of Insider Threats to Information Security Security." [Online]. Available: https://aisel.aisnet.org/acis2020
[24] R. Jayadi, "Understanding Employee Security Behavior In Using Information System Of Organizations: Evidence From Jakarta Greater Area, Indonesia," *J Theor Appl Inf Technol*, vol. 30, no. 12, 2022, [Online]. Available: www.jatit.org
[25] G. Narayana Samy *et al.*, "Multidimensional Insider Threat Detection Model For Organization," *J Theor Appl Inf Technol*, vol. 31, p. 20, 2021, [Online]. Available: www.jatit.org
[26] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," *Journal of Information Security and Applications*, vol. 40, pp. 247–257, Jun. 2018, doi: 10.1016/j.jisa.2017.11.001.
[27] J. R. C. Nurse *et al.*, "Understanding insider threat: A framework for characterising attacks," in *Proceedings - IEEE Symposium on Security and Privacy*, Institute of Electrical and Electronics Engineers Inc., Nov. 2014, pp. 214–228. doi: 10.1109/SPW.2014.38.
[28] A. A. Qashqari, A. M. Munshi, H. A. Alturkstani, H. T. Ghwati, and D. H. Alhebshi, "The Human Factors and Cybersecurity Policy."
[29] A. L. Beena and S. Humayoon Kabir, "Information Security Insider Threats in Organizations and Mitigation Techniques," in *2019 International Conference on Recent Advances in Energy-Efficient Computing and Communication, ICRAECC 2019*, Institute of Electrical and Electronics Engineers Inc., Mar. 2019. doi: 10.1109/ICRAECC43874.2019.8995088.
[30] I. Hilmi, E. Ivan, A. Özlem, and T. T. Tas¸seven, "Minimizing Insider Threat Risk with Behavioral Monitoring and Society," *Review of Business: Interdisciplinary Journal on Risk and Society*, vol. 38, no. 2, pp. 61–73, 2018.
[31] M. Omar, "Insider threats: Detecting and controlling malicious insiders."
[32] F. L. Greitzer *et al.*, "Unintentional insider threat: Contributing factors, observables, and mitigation strategies," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, IEEE Computer Society, 2014, pp. 2025–2034. doi: 10.1109/HICSS.2014.256.
[33] K. Kisenasamy, S. Perumal, V. Raman, and B. S. M. Singh, "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*, vol. 13, pp. 236–251, Mar. 2022, doi: 10.1007/s13198-021-01378-3.
[34] A. R. Marbut and P. D. Harms, "Fiends and Fools: A Narrative Review and Neo-socioanalytic Perspective on Personality and Insider Threats," *J Bus Psychol*, vol. 39, no. 3, pp. 679–696, Jun. 2024, doi: 10.1007/s10869-023-09885-9.
[35] X. Liu, Q. Li, and C. Sonali, "Social engineering and insider threats," in *Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2017*, Institute of Electrical and Electronics Engineers Inc., Jul. 2017, pp. 25–34. doi: 10.1109/CyberC.2017.91.
[36] P. D. Harms, A. Marbut, A. C. Johnston, P. Lester, and T. Fezzey, "Exposing the darkness within: A review of dark personality traits, models, and measures and their relationship to insider threats," *Journal of Information Security and Applications*, vol. 71, Dec. 2022, doi: 10.1016/j.jisa.2022.103378.
[37] J. Bedford and L. van der Laan, "Operationalising a framework for organisational vulnerability to intentional insider threat: the OVIT as a valid and reliable diagnostic tool," *J Risk Res*, vol. 24, no. 9, pp. 1180–1203, 2021, doi: 10.1080/13669877.2020.1806910.
[38] M. T. Whitty, "Developing a conceptual model for insider threat," *Journal of Management and Organization*, vol. 27, no. 5, pp. 911–929, Sep. 2021, doi: 10.1017/jmo.2018.57.
[39] L. Hadlington, "The 'human factor' in cybersecurity: Exploring the accidental insider," in *Psychological and Behavioral Examinations in Cyber Security*, IGI Global, 2018, pp. 46–63. doi:

10.4018/978-1-5225-4053-3.ch003.

[40] M. Dupuis and S. Khadeer, "Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat," in *RIIT 2016 - Proceedings of the 5th Annual Conference on Research in Information Technology*, Association for Computing Machinery, Inc, Sep. 2016, pp. 35–40. doi: 10.1145/2978178.2978185.

[41] F. L. Greitzer *et al.*, "Developing an Ontology for Individual and Organizational Sociotechnical Indicators of Insider Threat Risk".

[42] M. Button, "Editorial: economic and industrial espionage," Mar. 01, 2020, *Palgrave Macmillan Ltd.* doi: 10.1057/s41284-019-00195-5.

[43] H. Sepehrzadeh, "A method for insider threat assessment by modeling the internal employee interactions," *Int J Inf Secur*, vol. 22, no. 5, pp. 1385–1393, Oct. 2023, doi: 10.1007/s10207-023-00697-9.

[44] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," Sep. 01, 2020, *MDPI AG*. doi: 10.3390/electronics9091460.

[45] E. © Shaw, L. Sellers, and E. Shaw, "Application of the Critical-Path Method to Evaluate Insider Risks".

[46] B. Liu Hua Yeo and J. Banfield, "Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis."

[47] C. Joshi, J. R. Aliaga, and D. R. Insua, "Insider Threat Modeling: An Adversarial Risk Analysis Approach," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1131–1142, 2021, doi: 10.1109/TIFS.2020.3029898.