Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INSIDER THREATS: PROFILING POTENTIAL MALICIOUS ATTACKS, SEVERITY AND IMPACT

[1]ZUL-AZRI IBRAHIM, [2]FIZA ABDUL RAHIM, [3]ANIS ALIAH 'ALAUDDIN, [4]NORZIANA JAMIL, [5]HARIS ISKANDAR MOHD ABDULLAH

[1,3,4,5] College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia

[2]Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia

[1,2] Institute of Informatics and Computing Energy, Universiti Tenaga Nasional, Malaysia

E-mail: [1]zulazri@uniten.edu.my, [2]fiza.abdulrahim@utm.my, [3]anis.aliah@uniten.edu.my, [4]norziana@uniten.edu.my, [5]haris.iskandar@uniten.edu.my

ABSTRACT

The insider threat that organizations and cooperation face today is a real and serious issue that has become increasingly difficult to address as time has passed. More complex approaches must be researched and developed for reliable recognition, detection, and response to insider threats. One way to achieve this is by identifying and classifying diverse viewpoints of insider threats. Various studies focused on comprehending and mitigating insider threats by developing different taxonomies and terminologies relating to insiders, insider threats, and insider attacks. However, few are concerned about the severity and impact of insider threats to an organization. Therefore, this paper proposes a taxonomy for profiling potential malicious attacks, highlighting severity to determine the impact of insider threats and the prioritization of vulnerability remediation activities.

Keywords: *Insider threat, Insider Threat Detection, Taxonomy, Severity, Impact*

1. INTRODUCTION

An insider threat is a security risk that arises within the targeted company. It usually involves a current or former employee or business colleague who has authorized access to sensitive information or privileges within the organization's network but intentionally or unintentionally causes harm to the organization [1]. Although insider threats have been on the rise throughout the years, they still are one of the most underestimated aspects of cybersecurity. According to a survey [2], insider security incidents increased by 47% between 2018 and 2020, while the cost of insider threats grew by 31%. Furthermore, 60% of data breaches are caused by insider threats.

With the rising issue of insider threats over the years, it should be significantly taken into account to identify and classify various perspectives of insider threats. In their preliminary study, Nasser et al. [3] provide a taxonomy classification of hybrid insider threats to be used effectively to detect inside threats. [3]. Their later study revised the taxonomy to a descriptive category that focuses more on insider and insider threat detection [4]. Given that there has already been much research done on insider threat identification, the problem persists in modern society. We noticed that less effort had been made to abide by the severity of insider threats to one's organization. Moreover, classifying severity in insider threat detection should also be considered vital as it can identify which components should have been prioritized in mitigating insider attacks and vulnerabilities. Thus, this study presents a taxonomy comprising its perpetrator, insider, attack detection, and severity category.

The rest of this paper is laid out in several sections. Section 2 discusses related studies regarding insider threats and insider attacks, including taxonomies, detection methods, and analysis. Section 3 introduces the proposed taxonomy, and Section 4 concludes the paper and offers suggestions for future research.

2. RELATED WORKS

Insider threat research has gotten a lot of attention due to its impact on many organizations. Various researchers focus on understanding and mitigating this issue by coming out with various taxonomies and terminologies regarding insiders, insider threats, and insider attacks. The summary of all mentioned or reviewed properties related to insiders is tabulated in Table 1. Table 2 shows the summary of dimensions for insider threat detection.

Nasser *et al*. [3], in their preliminary study, propose a taxonomy of insider threats with terminologies that cover the entire insider threat field from objects (internal information) to subjects (insiders). The proposed taxonomy guides future research into insider threats, particularly insider threat detection and log files. However, in 2020, Nasser *et al*. [4] came out with a more precise taxonomy covering two perspectives of insider threats: insider and insider threat detection. The structural taxonomy provides future researchers with an extensive view and deep understanding of insider threats and how to detect them. Their studies and reviews contributed the most to our proposed taxonomy.

Likewise, Homoliak *et al.* [5] provide an insight into insiders and IT where they mentioned that one of the most challenging attack models to deal with in practice is insider threats. They prepare a structural taxonomy for a thorough literature review that provides a systematization of knowledge in insider threat research (based on their studies and 5W1H questions) while leveraging existing grounded theory. They present their taxonomy into two insider types which are malicious and unintentional.

There are various fields affected by insider threats and possible attack schemes. For example, Farsi *et al.* [6] developed a taxonomy focusing on security threats and associated techniques in a cloud computing environment. Another study by Mamchencko and Sabanov [7] investigates an adequate prediction of USB-based attack vectors to assess the relevance and sufficiency of applying the well-known protection means.

Table 1: Summary of Dimensions for Insider

Dimension	Characteristic	Mentioned / Reviewed by	Total Papers
Insider Access	Physical	[3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], and [14]	12
	Network	[3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], and [17]	15
	Host-based	[7], [8], [10], [11], [12], [15], [16], and [17]	8
	Hybrid	[5], [9], and [15]	3
Insider Motivation	Personal	[3], [4], [5], [14], [15], [18]	5
	Political	[3], [4], and [5]	3
	Financial	[3], [4], [5], [14], and [17]	5
Type of Insider	Unintentional	[3], [4], [5], [16], [17], [18], and [19]	7
Insider Profiling	Espionage	[4], [5], [8], [16], and [19]	5
	Fraud	[4], [5], [8], [11], [14], [16], [17], [18], and [19]	9
	Theft of Intellectual Property	[4], [5], [14], [16], [17], [18], and [19]	7
	Sabotage	[4], [5], [6], [8], [11], [14], [15], [16], [17], [18], and [19]	11
Insider Intentions	To gain access to system resources	[3], [4], [5], [6], [7], [8], [10], [11], [16], and [20]	10
	To cause malfunction	[5], [7], [9], [10], [11], [12], [16], and [19]	8
	To delete information	[5], [6], [7], [10], [15], [16], and [17]	7
	To steal	[3], [4], [5], [7], [8], [10], [11], [15], [16], [17], and [19]	11
	To modify	[3], [4], [5], [6], [7], [8], [9], [10], [14], [15], [16], [17], [19], and [20]	14
	To destroy	[4], [5], [7], [8], [9], [11], [14], [15], [16], and [20]	10
Attack Method	Information Exchange	[3], [7], [8], [10], [20], [21], and [22]	7
	User Command	[3], [4], [5], [8], [10], [15], [16], and [23]	8
	Exploitation	[3], [4], [5], [7], [8], [10], [11], [14], [15], [17], [20], and [23]	12
	Script	[3], [7], [8], [10], [11], [15], [20], and [23]	8
	Toolkit	[3], [4], [5], [8], [10], [15], [16], and [17]	8
	Autonomous Agent	[3], [8], [10], and [11]	4
	Probing	[3], [7], [8], and [10]	4
	Scanning	[3], [6], [7], [8], [10], [12], [14], [16], and [20]	9
	Social Engineering	[3], [4], [5], [8], [10], [11], [14], [16], [17], [18], [20], [23], and [24]	13

Aldawood *et al.* [8] developed an improved taxonomy for social engineering attacks to facilitate the development and implementation of countermeasures at both human-based and technology-based levels. In another study, Sharma *et al.* [9] conducted a 3-Dimensional analysis of cyber-physical system attacks to develop more secure products and align the security procedures across various application domains to protect against cyber-physical system attacks.

Due to the sheer complexity of the insider threat problem, much of the prior research has concentrated on modelling the problem and developing framework approaches to solving the issues revealed through modelling.

However, from all the research papers related to insider threats we studied, we found that few of them concern the severity of insider threats on an organization, as listed in Table 2. Therefore, our primary contribution to this review is the addition of the severity category in our taxonomy.

Table 2: Summary of Dimensions for Insider Threat Detection

Dimension	Characteristic	Mentioned / Reviewed by	Total Papers
Insider Threat Detection Methodology	Anomaly	[3], [4], [5], [6], [14], [15], [16], [24], and [25]	9
	Hybrid Classification	[4], [5], [16], [20], [21], [22], [24], and [25]	8
	Signature / Misuse-based	[3], [4], [5], [14], and [15]	5
	Rule-based	[4], and [14]	2
	General (Hypothesis-Based)	[5], and [14]	2
Insider Threat Indicator	Deliberate Markers	[3], and [16]	2
	Errors	[3], [5], [15], [16], [18], and [24]	6
	Patterns	[3], [5], [14], [16], [18], [20], [23], [24], and [25]	9
	Verbal Behaviour	[3], [4], [5], [14], [15], [16], [17], [18], and [24]	9
	Personality Traits	[3], [4], [5], [15], [16], and [17]	6
Insider Threat Data Source	Computer Usage Activities Log	[3], [4], [5], [8], [12], [14], [15], [16], and [17]	9
	Database	[5], [12], [13], [14], [16], [20], [21], [24], and [25]	9
	Network Traffic	[3], [5], [8], [9], [12], [14], [16], [20], [23], and [24]	10
	Email Content	[3], [4], [5], [8], [11], [12], [14], [15], [16], and [17]	10
	Documents	[5], [8], [16], [17], [21], and [26]	6
Affected Security Objective	Confidentiality	[3], [4], [5], [6], [7], [14], [15], [16], [17], [20], and [24]	11
	Integrity	[3], [4], [5], [6], [7], [14], [15], [16], [17], [20], and [24]	11
	Availability	[3], [4], [5], [6], [7], [9], [14], [15], [16], [17], [20], and [24]	12
Impact	Network	[3], [4], [6], [7], [8], [9], [10], [11], [12], [14], [17], [18], [20], and [24]	14
	Physical	[3], [4], [6], [7], [8], [9], [10], [11], [12], [14], [17], [18], and [20]	13
	Psychological	[6], [7], [8], [14], [18], and [20]	6
	Economic / Financial	[4], [7], [8], [11], [14], [15], [17], and [20]	8
	Political	[4], [7], and [14]	3
	Reputational	[4], [7], [8], [11], [14], [15], and [17]	7
Scope	Local	[8], [14], [17], [19], [20], and [27]	6
	Global	[14], [17], [19], [20], and [27]	5
Severity Level Contemplation	Low, Medium, High, Critical	[6], [7], [8], [9], [12], [17], [18], and [25]	8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. PROPOSED TAXONOMY

This literature review on insider threats was based on secondary data resources obtained from journals, conference papers, and books summarized in developing the proposed taxonomy, as illustrated in Figure 1. From the classification of insider threats taxonomy developed by [4], two main categories are adopted in the proposed taxonomy: *Insider* and *Insider Threat Detection*.

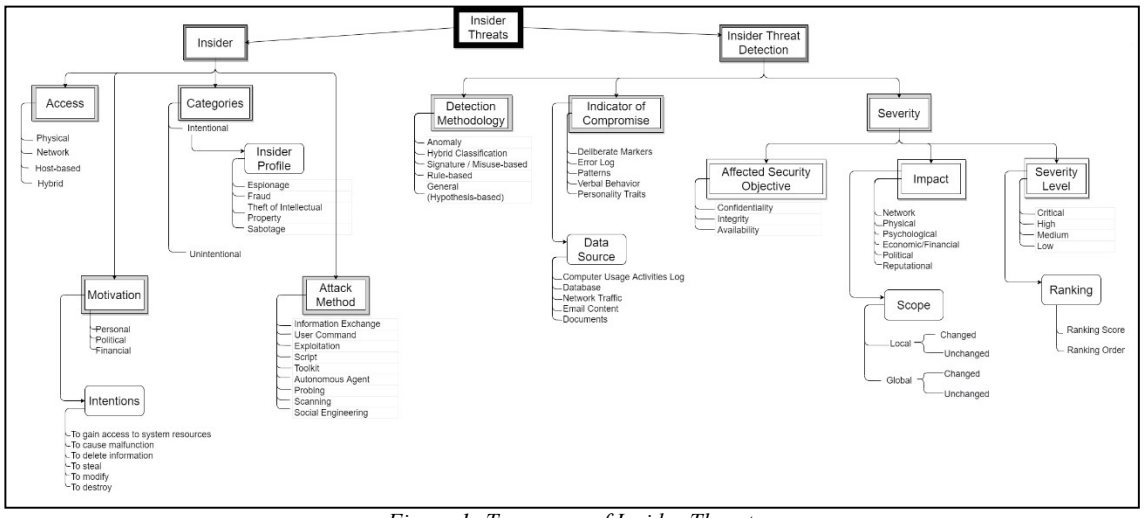

Figure 1: Taxonomy of Insider Threats

3.1 Insider

An *Insider* is an individual within an organization who has special knowledge or access to confidential information. For instance, a potential attacker derived from within an organization has authorization to areas or restricted information. This category includes *Access, Categories, Motivation, Intentions,* and *Attack Method*.

3.1.1 Access

Insiders naturally have authorized access within their roles to specific categories, allowing them to pose threats. *Access* can be categorized into *Physical*, *Network*, *Host-based*, and *Hybrid* in the proposed taxonomy. In more detail, *Physical Access* is when someone can access the company's department, facilities, and even their IT infrastructures. By possessing this access, insiders may find privacy-sensitive information that can be used to conduct authorized misuse actions, both intentionally or unintentionally [3]. Malicious insiders can exploit physical security vulnerabilities that can cause severe damage to organizations. They can also conduct mischievous actions to infiltrate data or steal devices.

Network Access involves insiders who have access to the company's secure network or systems. Insiders can misuse their access to data systems to steal intellectual property to commit fraud. Indeed, intrusion detection systems are vulnerable to internal attacks when intruders have authorized access inside a network or computer system [28]. Other methods for undermining an organization's reputation include leveraging network traffic to send unsolicited e-mails, denial-of-service (DoS) attacks and malware propagation.

Host-based System Access can be referred to as a hierarchical communications system managed by a central computer. It involves the operation mainly carried out by software in the computer rather than in a peripheral device. Host-based access describes insider access to host-based domains. For example, authorized insiders have access to monitored or modified activities of employees by tracking system calls at the operating system level, such as using logging tools [15]. Malicious insiders can bypass or disable the logging tools for their benefit by having this access.

Lastly, *Hybrid Access* describes insiders with access to a hybrid environment and infrastructures. Hybrid can be explained as a combination of on-site and, in the cloud, publicly or privately. They can work jointly together and could be managed with one set of policies. This feature domain can contain many insider activities such as file operations, e-mails, websites, etc. [15]. In addition, hybrid infrastructure requires different tools to manage the different environments. By having this access, malicious insiders may exploit the complexity of

this domain to their advantage, such as endangering and controlling critical data.

3.1.2 Categories

There are different types of insiders and can be categorized into two kinds: *Intentional* and *Unintentional*. An *Intentional* insider is a malicious employee who uses their authority to pose threats to their organization. The *Unintentional* type refers to an existing employee who unintentionally harms the organization or increases the possibility of future risk to their organization. Typically, the unintentional type does not intend to harm their company, but their careless action can cause one. For example, an employee downloading malicious content from the internet or error can cause system interruption.

3.1.2.1 Insider Profile

Insider Profile is obtained through behavioural data of intentional insiders because most insider threat attacks are deliberate. *Espionage*, *Fraud, Theft of Intellectual Property*, and *Sabotage* are the four types of *Insider Profiles*. *Espionage* is an act of spying on foreign entities to obtain classified or private information [16]. It includes the intentional destruction of a company's physical or logical resources so they can't be utilized [3], [29]. A masquerader is one example of espionage. It describes an external attacker posing as an authorized user to obtain unlawful access and authority to do malicious activities. Likewise, a masquerader can also be an attacker who does social engineering to persuade a legitimate insider to give up important information or access to a service or system, such as pretexting.

Fraud explains an employee's fraudulent action. Greed or financial problems are common motivators that lead to *Fraud*, and this form of crime is usually long-term. [5]. These *Fraud* criminals are also known as traitors of organizations that have access to critical data. These people are always looking for space and opportunities to use such data. They can also act violently using verbal harassment and other disruptive behaviour [18].

Theft of Intellectual Property describes taking someone's or an organization's ideas, inventions, creative output, or other intellectual property. *Theft of Intellectual Property* has many consequences for organizations, including a loss of competitive advantage, reputational damage, a delay in corporate growth, and customer trust.

Lastly, *Sabotage* happens when an organization's resources are intentionally destroyed so they can't be used. *Sabotage* can happen whether by a former employee with network access bent on *Sabotage* or even a foolish employee or associate who clicks on phishing links while using company devices. *Sabotage* can impact both physical and logical damage.

3.1.3 Motivation

It is essential to define insider threat's motivation and purpose for mitigation strategies. *Insider Motivation* is divided into three categories; *Personal*, *Political,* and *Financial*.

Personal Motivation is a type that can come in various forms but mostly in blackmail form [4]. The main target of this behaviour is someone who holds personal secrets which they do not want others to know. The attacker then offers some ransom bargains and threatens to disclose the personal secrets if the target does not want to cooperate. Many persons and organizations may face significant difficulties as a result of this. Another example of this motivation is disgruntled employees, consisting of current employees or unhappy former employees [3].

Political Motivation occurs when the attacker has a strong political view that urges everyone to have the same idealism. If other employees hold different opinions and actions, the attacker will cause harm when the opportunity arises or even collaborate with malicious individuals or organizations. Terrorist is a prime example of political agenda. Terrorism is an extreme/violent act to uphold political beliefs by causing severe damage that results in harm and even loss of life. Such behaviour can severely impact an organization's reputation and affect psychological well-being by causing stress, trauma, anxiety and personal insecurities [30].

Financial Motivation is a powerful force that can push some people to act in ways that no one could have predicted. It involves motivating or directing someone with money or anything associated with luxury to do malicious activities.

3.1.3.1 Insider Profile

In the proposed taxonomy, *Intention* is sub-*characteristic* for *Motivation* to describe the action taken by the insider based on the motivation's perspective. Although the terms motive and intent are sometimes used interchangeably, they are two separate concepts. Motive is more concerned with the attacker's underlying reasons for committing a crime. On the contrary, the intent is concerned with the attacker's desire to carry out the actions connected to the offence.

There are six elements under *Intentions*: *To gain access to system resources*, *To cause malfunction*, *To delete information*, *To steal*, *To modify* and *To destroy*. Each insider's motivation may contain the same intention. For example, a disgruntled insider may alter critical data to harm an organization's reputation. Another example is an insider who, motivated by financial gain, may launch an attack by modifying data to gain money from competitive cooperation.

3.1.4 Attack Method

An insider could use many various techniques to carry out an attack. In the proposed taxonomy, attack methods are classified into nine categories: *Information Exchange*, *User Command*, *Exploitation*, *Scripts*, *Toolkit*, *Autonomous Agent*, *Probing*, *Scanning*, and *Social Engineering*. An insider can utilize *Information Exchange* methods such as getting information from a user by inducing an attack (e.g., social engineering) or obtaining information from attackers [3], [31] via computer networks and telecommunications [4]. The attack method by *User Command* entails various operations that are entirely based on simple commands that legitimate users can run from the insider's computer account. Most of these incidents are undetectable by intrusion detection software [3], [32].

Exploitation can frequently occur as insiders are generally aware of their weaknesses and might exploit them. Exploiting physical security vulnerabilities is also a concern as an insider has access to various authorized and restricted areas and processes. Insiders planned to detonate a logic bomb by modifying production *Scripts* to perpetrate their attacks [33]. A logic bomb is malicious software that creates a backdoor account that allows the script to run. It is activated on the host network when particular criteria are satisfied.

The *Toolkit* is a software package containing a range of harmful or obfuscating programs regularly distributed on hacker websites [31]. While *Autonomous Agents* are software programmes that respond to states and events in their environment without direct instruction from the agent's user or owner, they work on the owner's behalf [34]. *Probing* is the process of gaining access to a target [31] via a known or potential weak point to determine its characteristics and vulnerabilities.

Scanning can work by continuously sending requests for information to learn about the vulnerabilities of the computer or the network [3], [31]. Finally, *Social Engineering* involves coercing employees into performing actions or disclosing confidential information that will be utilized maliciously to breach the company's network [35]. It employs psychological techniques to persuade users to make security mistakes or disclose critical information.

3.2 Insider Threat Detection

The second category is *Insider Threat Detection*, which describes the process and technology used to *detect* insider threats. Three elements have been identified under *Insider Threat Detection*: *Detection Methodology*, *Indicator of Compromise* and *Severity*.

3.2.1 Detection Methodology

A methodology is a procedure or approach used to find, select, process, and analyze a specific subject. *Anomaly Detection, Hybrid Classification,* Signature-*Based Detection, Rule-Based Detection*, and *General-Based Detection* are the five categories used to categorize *Detection Methodology.*

Anomaly Detection or outlier analysis is a data mining step that identifies unusual data points, events, or/and observations that differ from the predicted behaviour of a dataset. The irregularities discovered by this technique can be used to identify intrusion attacks [36]. A study has been conducted on an evaluation process for different machine learning techniques on the CERT Insider Threat test dataset to detect insider threats [37].

The *Hybrid Classification* method is relied on instance filtering to achieve a high level of accuracy while keeping the learning outcomes simple to comprehend. Even though misclassification examples are often dismissed as noise, they can include useful information for identifying the class values of other instances [38]. Decision tree induction and a Naïve Bayesian classifier are examples of algorithms used.

Signature-based or misuse-based detection is a process for establishing a unique identifier for a known threat to be identified in the future. The process takes place by providing the system with signatures of previous attacks. The system then detects new attacks by comparing signatures to those of previously identified attacks [15].

General-Based Detection used a hypothesis to detect insider threats. This methodology includes a three-tier conceptual model: hypothesis (top layer), measurement, and real-world (bottom layer). An observer or analyst would look at the model from the top and approach it in a bottom-up or top-down approach [14]. Measurements are being deduced

from real-world elements in a bottom-up approach. By recording attributes and behaviour to suggest insider intentions, these measurements can develop an insider profile. It will then generate a sub-hypothesis (low-level hypothesis) from which a future/more parent hypothesis can be constructed.

In comparison, the top-down approach begins when an analyst or observer has concern or suspicion about a particular person. This method can also be applied to a "what-if" scenario. The analyst will often have multiple sub-hypotheses and alerts and will later employ the available data from the measurements tier. As a result, the probability of the hypothesis being true would be the model output.

3.2.2 Indicator of Compromise

An indicator of compromise is a piece of information that can be used to identify potentially malicious activity on a system or network. By *compromising* potential risk indicators, organizations can detect attacks and act fast to avoid any unwanted activities by preventing attacks in the early stages by monitoring for indicators of compromise. These indicators are observable and reportable behaviours that indicate individuals who may be more likely to become a threat. We discussed five indicator categories in this section: *Deliberate Markers, Error Log, Patterns, Verbal Behaviour,* and *Personality Traits.*

Deliberate Markers are those left by attackers with the intent of making a statement. The magnitude and obvious markers might vary; therefore, discovering the smaller, less noticeable ones before a major attack should be the top priority for anyone seeking to spot them [39]. *Error Log* describes a record of critical errors that the application, operating system, or server encounters while in use. Error logs are extremely valuable for diagnosing and maintaining systems, servers, and even networks in many circumstances.

Patterns of insider attack can be found in the correlated usage of the computer system. These patterns may not be visible on a single system, but the fact that they appear on numerous systems can reveal the intents of a potential criminal [39]. On the other hand, insider threat data is usually continuous, and the pattern of threats changes over time [4]. *Verbal Behaviour* indicates insider manners, whether it is the expression of aggression, unusual enthusiasm, or disgruntlement [39]. A potential malicious insider may express physical or verbal dissatisfaction to damage the organization. Lastly, *Personality Traits* reveal potential ethical issues regardless of their thoughts, expressions, feelings, and behaviours. These basic characteristics can be quite useful in predicting insider attacks by looking at individuals' consistency and stability in their work.

3.2.2.1 Data Source

Insider attack signs can be found in various places, including data sources. Data sources can be categorized into five types, *Computer Usage Activities Log*, *Database*, *Network Traffic*, *E-Mail Content*, and *Documents*.

As computers are widely used in a working environment, organizations can monitor their employees' activities by collecting private datasets using *Computer Usage Activities Logs*. This log can contain system information as well as user's activities such as logins, e-mails with tags such as user ID, access events, browser usage, process usage, removable device usage, activity code, timestamp, host PC ID, usage after normal working hours, and PC owner [16]. Organizations can use the recorded log to detect potentially hidden behaviour like destruction, misuse, corruption, and theft [16].

Meanwhile, *Databases* remain the most prevalent data sources, serving as the primary storage for data in every industry. As a database contains data records or files information about sales transactions and/or interactions, Mathew et al. [40] propose a solution to address database management security problems against the insider threat. Using the S-vector technique, the proposed data-centric approach employs user access model patterns to profile users' data points and generate the numeric characteristics' min, max, mean, median, and standard deviation. The total count and number of distinct values are calculated using the non-numeric attribute.

Network Traffic can also be used as a data source for insider threat indicators by analyzing the ability of malicious behaviour through a network connection and HTTP requests [41]. Network connections and HTTP request logs represent the network traffic that characterizes IP network flow and individual HTTP requests and responses. Network connections contain TCP connection log information that is related to network flows, including the size of traffic sent over the connections, the total number of connections and the average duration of connections per host time. HTTP request logs and HTTP headers contain information about queries cached in a local database [41]. Thus, possible causes of any

abnormal activities found in the network traffic can also be triggered by insider threats.

Text exchange through e-mails or chat messages can also give away any malicious intent of someone against their organizations or targeted employees. Hence, *E-Mail Content* analysis and social network analysis needed to be done to detect insider threats involving collaborating traitors. One of the possible datasets that can be used is the Enron e-mail dataset [5].

Lastly, *Documents* can also be used as a source of information for insider threat indicators. Any irregular edit sequences to document information and works can cause intentional or unintentional insider threats. Furthermore, a stylometry application can also measure possible user traits for any obnoxious behaviour [41].

3.2.3 Severity

3.2.3.1 Affected Security Objective

CIA triad consists of three principles; *Confidentiality, Integrity* and *Availability,* which are crucial to information security because it helps organizations with complicated requirements, improve security posture and ensure business continuity [42]. As insiders possess authorized access to restricted areas and processes, keeping the CIA triad in check should be prioritized.

Confidentiality highlights the necessity to safeguard confidential and sensitive information from unwanted access [42]. This principle ensures that sensitive data is only accessed by authorized individuals and kept out of the hands of those who are not authorized to hold it.

Integrity ensures that the data available is accurate, authentic, and trustworthy. In other words, it ensures that the data has not been tampered with and can thus be trusted. Whether on a personal device, a storage device, a data centre, or the cloud, an organization must guarantee that its data is secured when in usage, transit, and stored [42].

Availability ensures that authorized users can access the systems, applications, and data when needed. To guarantee that critical business processes are not disrupted, networks, systems, and applications must be available [42].

Figure 2 shows that the most security propriety caused is availability disruption, composed of 12 out of 25 analyzed research papers. This finding is based on the fact that insiders can most likely cause interruption of services, applications, and data availability. The possible cause of this disruption can be both unintentional and intentional. For example, unintentional human errors in system maintenance can impact the performance and safety of equipment in many ways [42]. Hence, initiatives aimed at identifying and evaluating human error in maintenance are critical, as they can lead to the creation of a proper solution for human error reduction.

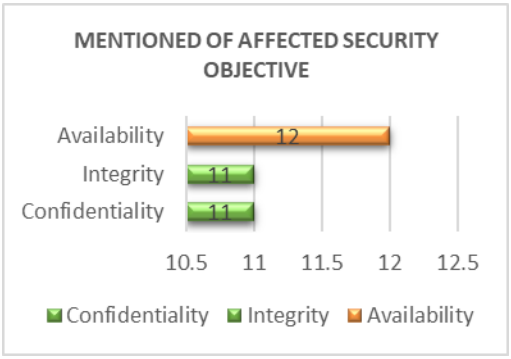

Figure 2: Mentioned Affected Security Objective Bar Chart

In addition, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks *can* be categorized as intentional attacks for availability disruption. These attacks can result in server outages, loss of productivity and loss of confidential data [43]. This can result in severe reputational and financial damage for an organization and psychological harm to employees, as they are pressured to get resources back online quickly [44].

3.2.3.2 Impact

Based on the studies of potential damage caused by the insider, we conclude that insider threats can also result in severe damage to each section of an organization. Thus, we classify this category into six types; namely *Network, Physical, Psychological, Economic or financial, Political* and *Reputational.*

Following a thorough review of the research articles, most papers mentioned insider threats could impact severe damage in the *Network* section, as seen in Figure 3. If the network sector is damaged, it can affect network equipment, operations, and productivity. An insider with authorized access to the network environment can launch a potential insider attack to disrupt the network, as discussed in Section 3.1.1. An analysis [4] supports this, stating that most insider threats are caused through network access. In the aftermath, system downtime can happen, which can cause severe damage to one's company. An example of the damage that can happen is the loss of productivity. As businesses today rely heavily on internet communications and services, losing

network connection may bring the entire workplace to a halt, from e-mail and software operations to task management and customer support systems. An unexpected server outage could shut down a manufacturing company's entire production line. If the missing services were part of a supply chain, this might have a long-term impact on productivity.

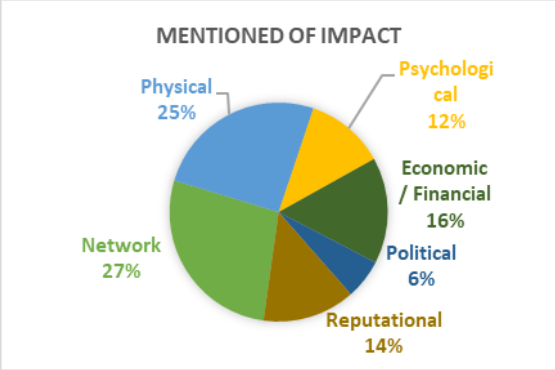

Figure 3: Mentioned Impact Pie Chart

Physical damage holds a high value of potential critical implications for an organization. Physical damage can cause tangible harm to a property that materially impairs its use, marketability, or value, whether it is caused intentionally or unintentionally. If physical vulnerabilities are not addressed, it will create unsafe working conditions and can lead to downtime losses. Furthermore, both network and physical locations can influence the severity of additional *Reputational*, *Political*, *Economic*, and *Psychological* sections. Therefore, organizations should tighten their security in both network and physical areas to reduce risks and damage.

3.2.3.2.1 Scope

The *Scope* is used to calculate whether the severity impact of insider threats only affected just locally within the organization or impacted thorough global aspect. The scope categorization is inspired by the Common Vulnerability Scoring System (CVSS) base metric group [45]. There are two main categories, namely, *Local* and *Global*, and both of these categories include *Changed* and *Unchanged*. If the Scope is modified, the severity is increased.

The severity of insider threats within the organization is assessed by *Local Scope*. Because *Local Scope* does not include impacted services between clients or other organizations, it only illustrates the influence of work processes and productivity locally.

Local Changed explains that a locally exploited vulnerability can have an influence on other systems. Insider threats that affect the organization's local database is considered to have a local changed scope. This is because the vulnerable component is the MySQL server database, where the attacker logs in to carry out the attack, and the impacted component is a remote MySQL server database (or databases) to which this database replicates. *Local Unchanged* describes the vulnerable and impacted local components are either the same or are managed by the same security authority [45]. For example, a negligent insider sends sensitive data to the wrong person via e-mail. This is considered *Local Unchanged* as the vulnerable components and impacted components are the same — the e-mail with sensitive data.

Global Scope considers affected customers, collaboration, enterprise, merchandise, global network, and services. *Global Changed* explains that an impact is caused beyond the exploitable component. For instance, a terrorist attack on an organization is considered *Global Changed* as the vulnerable components; physical and logical security vulnerabilities are different from impacted components. *Global Unchanged* describe only resources managed by the same security authority that can be impacted by an exploited vulnerability. For example, an irresponsible insider that neglects vulnerabilities found in the company's website can be considered *Global Unchanged* as the company's website serves as both vulnerable components and impacted components.

3.2.3.3 Severity Level

The severity level comes in four different levels: *Low*, *Medium*, *High*, and *Critical*. A *Low* level means the risk is low, and additional risk-reduction measures are not required. While the *Medium* level describes the risk may be acceptable, redesign or other *changes* should be considered if reasonably practical. Next, the *High* level indicates a not acceptable level. Further analysis should be carried out to provide a more accurate risk estimation. Lastly, the *Critical* level is the most concern and should be focused on immediately. This major event is most likely to cause severe damage that could ruin the organization.

3.2.3.3.1 Ranking

We categorized ranking into two types: *Ranking Score* and *Ranking Order*. Firstly, we calculate the severity of insider threats and tally them with other cases. We present the calculation in a ranking score for remarks and examination. After that, we continue the process by ranking them in order of severity to indicate which example cases are the most severe compared to others. By doing this,

organizations can determine their priority in mitigating insider attacks.

3.3 Comparison with other Taxonomies

This section describes the comparison of the proposed taxonomy with other developed taxonomies. As shown in Table 2, few studies focused on the severity of insider threats to an organization. In this paper, the proposed taxonomy highlights the importance of severity assessment to identify which components should be prioritized in preventing insider threats and vulnerabilities. Future studies may also incorporate the severity assessment of individual insider threat indicators and a detailed study of other insider threat indicator patterns, as suggested in [46].

4. CONCLUSION

Insider threats are one of the most common security concerns for organizations. Because of the significant impact on an organization, detecting the malicious insider threat is critical. However, organizations are either oblivious to the consequences of insider abuse or are afraid of losing their reputation and credibility if they divulge the details to the public.

This paper discussed related studies regarding insider threats and insider attacks, including taxonomies, detection methods, and analysis. A new taxonomy for profiling potential malicious attacks has been developed, highlighting severity to determine the impact of insider threats and the prioritization of vulnerability remediation activities.

In our future work, we will map the developed taxonomy on known real-world examples to demonstrate its compliance and validity in describing risks for selecting organizations' adequate protection solutions and strategies.

ACKNOWLEDGEMENT

Work presented in this paper is part of the research on Insider Threat: Understanding its Taxonomy, Various Approaches, Existing Gap and Future Research Direction Through Cyber Threat Analysis, which was partially funded by Universiti Tenaga Nasional BOLD Grant 2021.

REFERENCES:

[1] ID Watchdog, "Insider Threats and Data Breaches," 2022. https://www.idwatchdog.com/insider-threats-and-data-breaches/.

[2] D. G, "22 Insider Threat Statistics to Look Out For in 2022," *techjury*, 2022. https://techjury.net/blog/insider-threat-statistics/.

[3] M. N. Al Mhiqani *et al.*, "A new taxonomy of insider threats: an initial step in understanding authorized attack," *Int. J. Inf. Syst. Manag.*, vol. 1, no. 4, p. 343, 2018, doi: 10.1504/ijisam.2018.094777.

[4] M. N. Al-Mhiqani *et al.*, "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations," *Appl. Sci.*, vol. 10, no. 15, 2020, doi: 10.3390/app10155208.

[5] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," *ACM Comput. Surv.*, vol. 52, no. 2, 2019, doi: 10.1145/3303771.

[6] M. Farsi, M. Ali, R. A. Shah, A. A. Wagan, and R. Kharabsheh, "Cloud computing and data security threats taxonomy: A review," *J. Intell. Fuzzy Syst.*, vol. 38, no. 3, pp. 2529–2537, 2020, doi: 10.3233/JIFS-179539.

[7] M. Mamchenko and A. Sabanov, "Exploring the taxonomy of USB-based attacks," *Proc. 2019 12th Int. Conf. "Management Large-Scale Syst. Dev. MLSD 2019*, no. October 2019, 2019, doi: 10.1109/MLSD.2019.8910969.

[8] H. Aldawood and G. Skinner, "An Advanced Taxonomy for Social Engineering Attacks," *Int. J. Comput. Appl.*, vol. 177, no. 30, pp. 1–11, 2020, doi: 10.5120/ijca2020919744.

[9] M. Sharma, F. Gebali, and H. Elmiligi, "3-Dimensional Analysis of Cyber-Physical Systems Attacks," *2018 4th Int. Conf. Comput. Commun. Autom. ICCCA 2018*, pp. 1–5, 2018, doi: 10.1109/CCAA.2018.8777580.

[10] H. Hindy, E. Hodo, E. Bayne, A. Seeam, R. Atkinson, and X. Bellekens, "A taxonomy of malicious traffic for intrusion detection systems," *2018 Int. Conf. Cyber Situational Awareness, Data Anal. Assessment, CyberSA 2018*, pp. 1–4, 2018, doi: 10.1109/CyberSA.2018.8551386.

[11] J. Rastenis, S. Ramanauskaite, J. Janulevicius, A. Cenys, A. Slotkiene, and K. Pakrijauskas, "E-mail-Based Phishing Attack Taxonomy," *Appl. Sci.*, vol. 10, no. 7, pp. 1–15, 2020.

[12] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2019-Octob, no. Cic, 2019, doi: 10.1109/CCST.2019.8888419.

[13] L. Püschel, M. Röglinger, and H. Schlott, "What's in a Smart Thing? Development of a Multi-Layer Taxonomy," *2016 Int. Conf. Inf. Syst. ICIS 2016*, vol. 4801, 2016.

[14] P. Legg *et al.*, "Towards a conceptual model and reasoning structure for insider threat detection," *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 4, no. 4, pp. 20–37, 2013, doi: 10.22667/JOWUA.2013.12.31.020.

[15] R. A. Alsowail and T. Al-Shehari, "Empirical detection techniques of insider threat incidents," *IEEE Access*, vol. 8, pp. 78385–78402, 2020, doi: 10.1109/ACCESS.2020.2989739.

[16] A. Kim, J. Oh, J. Ryu, and K. Lee, "A review of insider threat detection approaches with IoT perspective," *IEEE Access*, vol. 8, pp. 78847–78867, 2020, doi: 10.1109/ACCESS.2020.2990195.

[17] A. Masood and A. Masood, "A Taxonomy of Insider Threat in isolated (air-gapped) Computer Networks," *Proc. 18th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2021*, pp. 678–685, 2021, doi: 10.1109/IBCAST51254.2021.9393281.

[18] F. L. Greitzer, J. Purl, D. E. Becker, P. J. Sticha, and Y. M. Leong, "Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2019-Janua, pp. 3202–3211, 2019, doi: 10.24251/hicss.2019.387.

[19] F. L. Greitzer, J. D. Lee, J. Purl, and A. K. Zaidi, "Design and Implementation of a Comprehensive Insider Threat Ontology," *Procedia Comput. Sci.*, vol. 153, pp. 361–369, 2019, doi: 10.1016/j.procs.2019.05.090.

[20] S. Berger, O. Bürger, and M. Röglinger, "Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy," *Comput. Secur.*, vol. 93, p. 101790, 2020, doi: 10.1016/j.cose.2020.101790.

[21] H. Gimpel, D. Rau, and M. Röglinger, "Understanding FinTech start-ups – a taxonomy of consumer-oriented service offerings," *Electron. Mark.*, vol. 28, no. 3, pp. 245–264, 2018, doi: 10.1007/s12525-017-0275-0.

[22] S. Berger, M. S. Denner, and M. Röglinger, "The nature of digital technologies - Development of a multi-layer taxonomy," *26th Eur. Conf. Inf. Syst. Beyond Digit. - Facet. Socio-Technical Chang. ECIS 2018*, no. February 2019, 2018.

[23] Z. Syed, A. Pädia, T. Finin, L. Mathews, and A. Joshi, "UCO: A Unified Cybersecurity Ontology," *AAAI Work. - Tech. Rep.*, vol. WS-16-01-, no. February, pp. 195–202, 2016.

[24] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy model for cyber threat intelligence information exchange technologies," *Proc. ACM Conf. Comput. Commun. Secur.*, vol. 2014-Novem, no. November, pp. 51–60, 2014, doi: 10.1145/2663876.2663883.

[25] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," *Proc. - 2017 Eur. Intell. Secur. Informatics Conf. EISIC 2017*, vol. 2017-Janua, pp. 91–98, 2017, doi: 10.1109/EISIC.2017.20.

[26] A. Strasser, "Delphi method variants in information systems research: Taxonomy development and application," *Electron. J. Bus. Res. Methods*, vol. 15, no. 2, pp. 120–133, 2017, doi: 10.25968/opus-1164.

[27] J. Jöhnk, M. Röglinger, M. Thimmel, and N. Urbach, "How to implement agile it setups: A taxonomy of design options," *Proc. 25th Eur. Conf. Inf. Syst. ECIS 2017*, no. June, pp. 1521–1535, 2017.

[28] W. Li, W. Meng, and L. F. Kwok, "Surveying Trust-Based Collaborative Intrusion Detection: State-of-the-Art, Challenges and Future Directions," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 1, pp. 280–305, 2022, doi: 10.1109/COMST.2021.3139052.

[29] T. Casey, "A Field Guide to Insider Threat," *Intel White Pap.*, no. October, p. 9, 2015.

[30] M. L. Gross, D. Canetti, and D. R. Vashdi, "Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes," *J. Cybersecurity*, vol. 3, no. 1, pp. 49–58, 2017, doi: 10.1093/cybsec/tyw018.

[31] A. Cummings, T. Lewellen, D. Mcintire, A. P. Moore, and R. Trzeciak, "Insider threat study: Illicit cyber activity involving fraud in the u. s. financial services sector," *Spec. Rep. CERT Progr.*, no. July, 2012.

[32] "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector." .

[33] D. M. Cappelli, T. Caron, R. F. Trzeciak, and A. P. Moore, "Spotlight On: Programming Techniques Used as an Insider Attack Tool," 2008.

[34] T. Bösser, "Autonomous Agents," *Int. Encycl. Soc. Behav. Sci.*, pp. 1002–1006, 2001, doi: 10.1016/B0-08-043076-7/00534-9.

[35] D. Wallen, "Social Engineering: The Insider Threat to Cybersecurity," *Cloud and Data Security*, 2019. https://spanning.com/blog/social-engineering-insider-threat-to-cybersecurity/.

[36] B. Steenwinckel, "Adaptive anomaly detection and root cause analysis by fusing semantics and machine learning," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11155 LNCS, pp. 272–282, 2018, doi: 10.1007/978-3-319-98192-5_46.

[37] M. Dosh, "Detecting insider threat within institutions using CERT dataset and different ML techniques," *Period. Eng. Nat. Sci.*, vol. 9, no. 2, pp. 873–884, 2021, doi: 10.21533/pen.v9i2.1911.

[38] T. T. Wong, N. Y. Yang, and G. H. Chen, "Hybrid classification algorithms based on instance filtering," *Inf. Sci. (Ny).*, vol. 520, pp. 445–455, May 2020, doi: 10.1016/J.INS.2020.02.021.

[39] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Comput. Secur.*, vol. 21, no. 6, pp. 526–531, Oct. 2002, doi: 10.1016/S0167-4048(02)01009-X.

[40] S. Mathew, M. Petropoulos, H. Q. Ngo, and S. Upadhyaya, "A data-centric approach to insider attack detection in database systems," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6307 LNCS, no. May, pp. 382–401, 2010, doi: 10.1007/978-3-642-15512-3_20.

[41] M. Mayhew, M. Atighetchi, A. Adler, and R. Greenstadt, "Use of machine learning in big data analytics for insider threat detection," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2015-Decem, no. September, pp. 915–922, 2015, doi: 10.1109/MILCOM.2015.7357562.

[42] Unitrends, "The CIA Triad and Its Importance in Data Security," *Backup, DR, DRaaS, Recovery, Security*, 2022. https://www.unitrends.com/blog/cia-triad-confidentiality-integrity-availability.

[43] B. Greevink, "What is a DDoS attack and what are the consequences?," 2018. https://www.trimm.nl/en/blogs/wat-is-een-ddos-aanval-en-wat-zijn-de-risicos#:~:text=A Distributed Denial of Service,can be started very easily.

[44] Kaspersky, "Distributed Denial of Service: Anatomy and Impact of DDoS Attacks," *2022*. https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work.

[45] Forum of Incident Response and Security Teams Inc., "CVSS v3.1 Specification Document," *2021*. https://www.first.org/cvss/specification-document.

[46] F. L. Greitzer and J. Purl, "The Dynamic Nature of Insider Threat Indicators," *SN Comput. Sci.*, vol. 3, no. 2, pp. 1–15, 2022, doi: 10.1007/s42979-021-00990-1.