Kwaghe International Journal of Engineering and Information Technology

ISSN : 1595-8035

Index: Harvard, Boston, Sydney University, Dimensions, Lens, ResearchGet Scilit, Semantic, Google Scholar, Base etc

https://doi.org/10.58578/KIJEIT.v2i3.7704

A Comprehensive Survey of Insider Threat Landscape and Detection Indicators

Fatai A. Akinsola[1], Francisca N. Ogwueleka[2], Uche M. Mbanaso[3]

[1,3]Nasarawa State University, Keffi, Nigeria; [2]University of Abuja, Abuja-FCT, Nigeria

akinsola@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Sep 15, 2025	Oct 6, 2025	Oct 18, 2025	Oct 23, 2025

Abstract

The persistence of insider attacks underscores the inadequacy of existing organizational defense strategies, particularly those that fail to prioritize the human element in cybersecurity planning. While external threats have traditionally dominated security frameworks, this study highlights the growing risk posed by internal actors due to the general absence of comprehensive insider threat strategies. Inadequate attention to insider threats can result in significant breaches, including data theft, information leakage, fraud, sabotage, and espionage. This study reviews the underlying factors and indicators that increase organizational vulnerability to insider attacks, categorizing various insider threat types and analyzing recent cases to illustrate their operational and reputational impacts. It also examines current tactics, frameworks, and best practices developed by cybersecurity professionals to counter this threat. Key detection indicators identified in the study reveal how insider activities may expand the attack surface, posing critical risks to digitally-enabled business operations. The findings offer practical guidance for cybersecurity practitioners, emphasizing the importance of integrating behavioral, organizational, and technological indicators into the design of insider threat

KIJEIT Journal is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

detection and prevention systems. The study also calls for ethical consideration in monitoring employee activities, advocating for a balance between threat mitigation and the preservation of individual rights, dignity, and workplace trust.

Keywords: Insider Threats; Cybersecurity; Organizational Vulnerability; Data Privacy; Risk Mitigation; Cyberattacks; Insider Risk Detection

Introduction

Cybersecurity incidents with costly and disruptive narratives continued to create fears and sometimes with lots of wrong ideas circulating. Hardly a day passes by without news about cyberattacks (Dacorogna & Kratz, 2023). The perpetrators are actors from within and outside the organizations playing disturbing roles in high-profile data breaches. The factors fueling cybercrime opportunities and rising insider threats incidents can be attributed to increased digitization, wide spread automation and popularization of mobile technologies (Hoffmann, 2020). This trend has led to frequent and costly occurrences of cyberattacks (Global Cybersecurity Outlook, 2022). Cyber threats can take many forms, data breaches, hacking, identity theft, ransomware, phishing, and many more. The risks and consequences of cyber threats can be severe and far-reaching on the social and economic well-being of the society (Agrafiotis et al., 2018). The study of insider threat detection and countermeasures is motivated by humongous degree of attacks that have the potential to endanger human existence (Homoliak et al., 2019). Thus, the challenge facing individuals, organisations, industries and the nation states is to have an effective strategy that will address cybersecurity perspectives not only from outside but from insiders as well.

The need to protect company sensitive data from insider attacks has become increasingly relevant in the light of recently released and disturbing statistics. According to the 2023 Insider Threat Report (Cybersecurity Insiders), the new normal of hybrid work methods, access to more cloud applications, and increasing economic uncertainty are driving insider risk to new levels (Holger, 2023). The research report indicated 74% of organizations agreed that insider attacks have become more frequent in the last 12 months. Subhani (2021) stated that humans are the least reliable security defense and are usually to blame when sensitive information is compromised. According to research by Standaford University Professor Jeff Hancock and security firm Tessian, 85% of security breach

incidents are caused by human error (Tessian, 2021; Tongkaw, 2019). Employee carelessness, such as using simple passwords, sharing passwords, leaving devices unlock after use, or indiscriminate connection to Wi-Fi have been found to contribute to the prevalence of insider attacks. Singleton (2021) reported that 60% of active technology threats resulted from malicious insiders, and 40% resulted from employee negligence.

Organisations are at risk from malicious insiders for various reasons, including retaliation against coworkers, conflicts with employees, dissatisfaction with the job or to help family and friends, including industrial/IT sabotage, or the pursuit of business advantage (Subhani, 2021). Insider threats can be more devastating just as external threats (Max, 2018). The disturbing statistics on the danger of insider threats is a trigger and a call for cohesive and pragmatic approach to managing insider attacks (Subhani, 2021).

To successfully deal with the risk of insider threat and adapt our activities to the new cyber reality, organisations should look at issues such as data protection and privacy in a completely new and fresh manner. Cybersecurity should therefore be prioritised in order to take advantage of digital transformation and the fourth industrial revolution. It is therefore imperative that urgent steps be taken to find innovative and more feasible solutions to prevent cyberattacks (Aslan et al., 2023).

Review of Related Studies

Cyber Threats

The rapid increase in the use of cyberspace has resulted in an exponential increase in cybercriminal activities (Humayun et al., 2020). A cyber security threat is a malicious actor that gains unauthorized access to computer networks or another person's or organization's network to damage, disrupt, or steal data (Abomhara & Køien, 2015). Cyber threats can originate from variety of sources such as hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

The common types or categories of cyber threats are malware, social engineering, supply-chain-attack, man-in-the-middle-attack, data breaches, denial-of-service, privilege escalation, hackers and insider threat (Aslan, et al., 2023; Abomhara & Køien, 2015). Cyberattacks has become more attractive and potentially more disastrous as our dependence on information technology increases (Jang-Jaccard, et al., 2014). Cyberattack is

an intentional move to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate, steal the data held within these systems or sabotage certain activities. Any individual, organized group, nation state can launch a cyber-attack from anywhere using one or more attack strategies.

Types of Insider Threats

A good place to start insider threat detection, mitigation or preventions strategy is to understand the different sources of threats or dangers namely natural phenomenon, human-induced and accident, system or technology failure (Snedaker, 2007). Organisations should consider sources of threat including the level of the threats when planning insider threat mitigation program. Snedaker (2007) identified three sources of threats, as follows:

a. Natural phenomenon: The threat can be both predictable and unpredictable and their impact can be small, big or catastrophic. Example of this can be climate related such as heavy rain, storms, hurricanes, fire or geographical threats such as earthquake, volcanic eruption and tsunami;

b. Human-induced: These threats are caused by humans and often intentional. Examples include armed attack, cyberattack, fire, explosion, riots, kidnapping, civil disobedience, and theft;

c. System, accident or technology failure: These threats are generally unintended. They include accident, infrastructure or system failures, dam failures, information systems failures, etc.

Knowing the characteristics or capabilities of insiders could aid organisations to appreciate the depth of the problem as well as to develop appropriate monitoring and mitigation strategies that is not only focused on technical measures but also on behaviuoral and phycological factors. Insider threats can be classified into four categories namely sabotage, data theft (of intellectual property), fraud, and espionage (Cappelli et al., 2012; Collins et al., 2016; Maasberg, 2015)). Greitzer (2019) identified five main types of insider threats which include insider sabotage, insider data theft/exfiltration, insider fraud, unintentional insider threat and workplace violence. Subhani et al. (2021) identified three insider types viz: traitor, masquerader and unintentional insider. Insider actions constitute a risk to organisation's information and information processing systems and the harmful

actions of the insiders are different for different insider threat types. The different types of insider threats are shown in Figure 1.

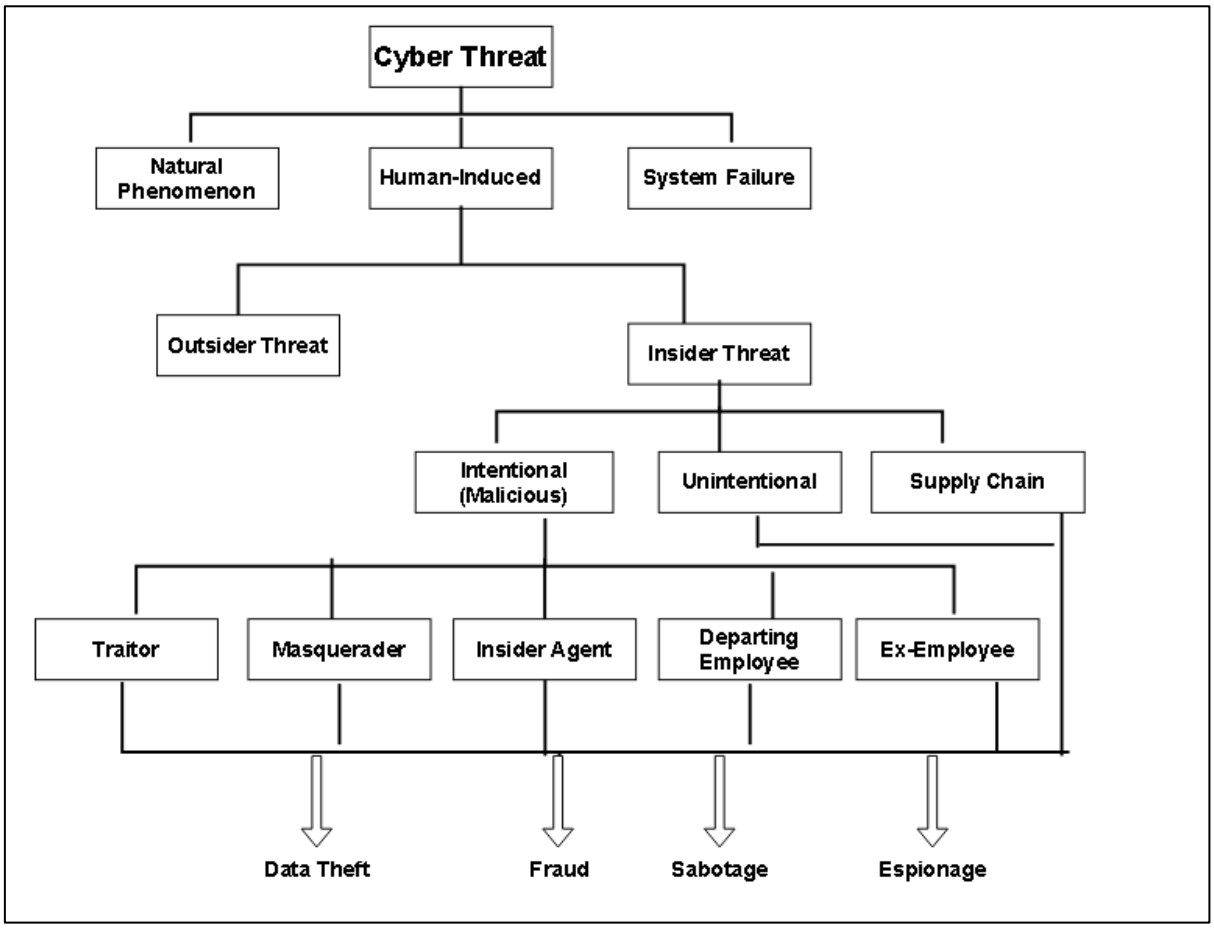


Figure 1: Cybersecurity Threats with Focus on Insider Threat (Greitzer, 2019)

The three main types of insider threats are:

i. Unintentional Insiders: The unintentional insider pertains to a current employee who unintentionally causes harm or increases the possibility of future harm to the organization (Al-Mhiqani et al., 2020). Unintentional insiders do not cause harm due to malicious intent but rather due to lack of knowledge or poor judgement (Greitzer, et al., 2019).

There are two types of unintentional insiders which include negligent and complacent insiders. Negligent insiders are employees or contract resources that put organisation's sensitive information at risk as a result of poor security culture such as exposing sensitive documents or misplacing data drives. Complacent insiders are employees who ignore basic security protocols like changing passwords regularly, updating

security patches or accidentally entering sensitive email information. Both negligent and complacent insiders are vulnerable to threats like email phishing.

ii. Intentional Insiders: Intentional insiders are employees who consciously and deliberately put the information asset of an organisation at a risk. Intentional insider attacks are usually caused by "disgruntled employees, activist, terrorists, organized crime, competitors, thieves, and irrational individuals" (Boakye-Gyan, 2021). The intentional insider is malicious in nature and can further be subdivided into traitor, masquerader, insider agent, departing employee and ex-employee.

Intentional insiders also referred to as malicious insiders can be divided into traitor, masquerader, insider agent, departing employee and ex-employee. These are employees who intentionally and deliberately compromise the confidentiality, integrity and availability of organisation's information. Saxena et al. (2020) described a malicious insider as an individual who intentionally misuse legitimate credentials maliciously to harm his organisation such as stealing confidential information for financial or personal gains. Malicious insiders do so because of different reasons which may include financial benefits or holding of grudges against their employer. Each of these categories of intentional insiders are explained in the following sections:

(a.) Traitors: Traitors, also known as misfeasors are users from within the organisation who use their access privileges to compromise the organisation's systems (Al-Mhiqani et al., 2020). According to Homoliak et al. (2019), traitors have full knowledge about the systems they work with on a daily basis, as well as the actual security policies. Traitors usually act on their own behalf, and therefore use their own credentials for malicious actions.

(b.) Masquerader: A masquerader is an external attacker who steals the legitimate identification of an insider and uses the stolen identity to impersonate the insider for malicious acts (Liu et al., 2018). Masqueraders have far less knowledge than traitors. They are attackers who steal the credentials of another legitimate user, and then use the stolen credentials for executing a malicious act on behalf of another user.

(c.) Insider agent: There have been cases where the insider had collaborated and sourced external agents with whom to instigate the attack against his employer (Rama, 2023).

(d.) Departing Employees: These are employees leaving the company voluntarily or involuntarily who may copy sensitive information or trade secret to help land a new job or to expose sensitive information about their employer out of revenge (Ostendorf, 2023).

(e.) Ex-employee: These are employees who left the organisation on unfavorable terms, such as termination or layoff, may harbor feelings of anger or resentment. They can pose significant insider threat risks for being disgruntled. Al-Mhiqani et al (2020) identified ex-employee as another level of insider.

iii. Supply Chain: Supply chain is a risk to the organisation's goods, services, information or systems and it results from individuals with authorised access to them. Suppliers, contractors, vendors, and other external service providers with some level of access can pose significant risk to the organisation. Boakye-Gyan (2021) noted that outsourcing can fragment or dilute protection controls leading to an increase in third party access and privilege akin to the insider.

Different circumstances lead to insider threats. The common insider threat types that people are concerned with are shown in Figure 2.

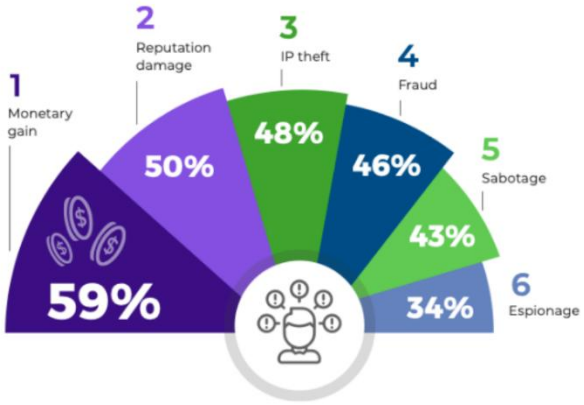


Figure 2. Percentage of insider attacks

(Source:www.cybersecurity-insiders.com 2023 Insider Threat Report)

i. Data Theft: This is a case of malicious insiders using the access they have to steal sensitive data such as customer information, intellectual property, or trade secret in order to sell for profit making or use to their benefits or gain competitive advance (Rakhi et al. 2025).

ii. Fraud: This involves manipulation of financial records or misuse of sensitive information to steal money from the organisation. Eamples include altering financial records, diverting

funds, stealing data to commit identity theft or sell it, and manipulating transactions or systems for private benefit (Maasberg, 2015).

iii. Sabotage: Sabotage refers to deliberate, harmful actions perpetrated by insiders such as an employee, contractor, or vendor with authorised access to organisation's information assets in order to damage the organisation's systems, infrastructure, reputation, or operations (Cappelli, et al 2015).

iv. Espionage: This is also known as spying. It is a situation when an insider is hired by other organisations or foreign agents or government to collect confidential information without the knowledge or consent of the company, typically for military, political, or economic advantage (Collins et al., 2016).

Insider Threat Cases and their Impacts

Intentional or unintentional acts of insiders could cause equally damaging impact such as sensitive data theft, data leakage or breach, or even supporting external attackers by creating backdoors to allow them gain illegal access to company's computer systems and networks (Alsowail & Al-Shehari, 2022). Recent research reports and statistics provide undisputable proof that insider threats constitute a worm ravaging several organisations today. The statistics highlights the seriousness, criticality and the urgent need to have a deliberate approach to mitigating the threats posed by insiders. Surveys of organisations in government and industry have indicated the threats posed by insiders compete with those posed by outsiders and that insider-motivated attacks are even more prevalent and costly (Boakye-Gyan, 2021). Alsowail & Al-Shehari (2022) opined that attacks from inside can be more serious than external attacks because insiders are authorised users who have legitimate access to organisation's information processing systems and sensitive information.

The severity of security breaches caused by insiders can be noticed from the following real-life incidents. The first example was the case of electric vehicle giant Tesla that suffered data breach orchestrated by two former employees who leaked sensitive personal data to a foreign media outlet (Ostendorf, 2023). The leaked information included names, addresses, phone numbers, employment records, and social security numbers of over 75,000 current and former employees. The insider breach also exposed other sensitive information of customers such as bank details and production secrets. The second example according to Morrow (2020) was an incident that involved Twitter (now called X) that fell

prey to social engineering using phishing attack as a vector. The attack led to the compromise of high-profile Twitter accounts. Attackers had sought information about internal systems and processes with some workers eventually fell for the scam and led the hackers to gain access to account support tools that helped them break into 130 Twitter accounts (Ostendorf, 2023). Another example is a case of careless Reddit employees acting as insider agent to cause harm that led to the stealing of credentials after engaging with a fraudulent landing page (Ostendorf, 2023). In June 2023, Raddit admitted a security breach where an employee was lured into interacting with a deceptive landing page, posing as an internal site, which granted attackers access to select Reddit systems. This incident compromised a database that contained email addresses and logs with user credentials dating back to 2007.

In addition, 1,154 actual insider threat incidents in Collins (2016) were reported by the U.S. Security Service and CERT. Such insider attack incidents have been classified into different categories: sabotage, fraud, theft, and miscellaneous. A number of 659 from the reported incidents fell under the category of fraud in which data were modified or deleted for the aim of personal gain, whereas 189 of the reported incidents fell under the category of theft, where intellectual properties of organisations were stolen. The rest of the reported incidents fell under the categories of sabotage and miscellaneous, where the aim was to disrupt business operations of organizations (Collins, 2016). Although some organizations have reported cases insider security breaches, other organisations have not for fear of negative impact such as damage to brand or reputation. The methods used by insiders to spread attacks have changed over time. Vulnerabilities in hardware, software, networks, physical assets are all commonly exploited to compromise organisation's security. These attacks are often spread through social engineering, phishing, malware, man-in-the-middle attacks. Some real-life incidents of insider attacks are summarised in Table 1.

Table 1. Threat Cases and their Impacts

Affected Entity	Year	Insider Type	Attack Method	Consequences
Tesla	2023	Malicious Insider	Sensitive personal data leaked	Exposure of sensitive personal data
Yahoo	2022	Departing Employee	Intellectual Property (IP) Download	Theft of 570,000 pages IP data
Apple	2022	Departing employee	Trade secrets stole while being poached	Gigabytes of confidential SoC information
Pegasus Airlines	2022	Unintentional insider	Cloud misconfiguration by a system administrator leading to data exposure	Exposure of Personally identifiable information (PII).
Cash App	2022	Disgruntled employee	A former disgruntled employee down-loaded the personal data of users of the mobile payment service Cash App	Personal data of 8.2 million customers leaked and legal actions taken against Cash App Investing and its partner.
SGMC	2021	Ex-employee	Data theft by a former SGMC employee	Client data leak
Ponemon	2022	Departing Employees	Confidential sales data stolen	Competitor enriched with stolen sales data
Twitter (now X)	2020	Malicious Insider	Social engineering	130 Twitter accounts hacked
Marriott	2020	Supply chain	Employees credentials exploited to hack a vulnerable application	5 million guest records stolen
Stradis Health care	2020	Disgruntled employee	Used a secret account he created while in employment before he was fired	Data loss (critical shipping data deleted

Related Work on Insider Threat Mitigation Frameworks

According to Modini et al. (2020), an insider threat program requires a comprehensive and multi-faceted approach. Ryan et al. (2013) defined an insider threat framework as some form of logical structure or model to guide an enterprise to organize information or activities to mitigate against an insider attack. Additionally, Balakrishnan (2015) characterized an insider threat framework as a mitigation approach that contains a meticulous plan with top management support and directed by policies, procedures, and controls with the main aim of reducing the risk related to insider threats to an acceptable

level. An effective insider threat program should be established to help organisations to detect, prevent, respond to as well as recover from and insider attack (Modini et al., 2020).

In recent years, the literature on insider threat mitigation framework has attracted much attention. Past studies have focused on one side of the problem or the other. While some were occupied with detection techniques (Sarhan & Altwaijry, 2022; Tang, 2016; Alsowail et al., 2020; Aldairi et al., 2019; Al-Mhiqani et al., 2020; Hu et al., 2019), others were biased towards mitigation (Homoliak, 2019; Alsowail & Al-Shehari, 2022; Alexander, 2018; Cappelli et al., 2010; Greitzer et al., 2009; Hunker & Probst, 2011; Rakan et al., 2022). To the best of our knowledge, there is no study on insider threat management that is all-encompassing with emphasis on critical elements of security such as governance and oversight, digital infrastructure identification, cybersecurity goals and objectives, vulnerability and indicators of threat evaluation, insider risk assessment, as well as a risk-based insider threat control selection.

Bilusich, et al. (2018) applied the concept of risk-based approach called security-in-depth (SID) for mitigating the risk of insider threats. The authors developed and applied a risk-based framework to model the spectrum of insider threat types, that could allow decision makers to prioritise security investment to achieve the greatest cost-benefit using residual risk as the performance metric. The technique was built on the concept of layered security where security layers can be applied to target specific parts of the threat kill chain. By having multiple layers, the perpetrator must defeat each security layer to be successful. The main achievement of the paper is that it allows decision makers to prioritise security investment to achieve the greatest cost-benefit using residual risk as the performance metric. The paper however, did not consider insider threat from the perspectives of individual, organisational or technical indicators that could serve as signals to potential insider attacks.

Alsowail & Al-Shehari (2021) proposed a unified framework that incorporates various context of insider threats - technical, psychological, behavioural and cognitive. The approach was based on a multitiered approach that encompasses pre, in and post-countermeasures to address insider threats. They considered multiple factors that surround the lifespan of insiders' employment, from the pre-joining of insiders to an organization until after they leave. The paper went beyond just technical monitoring at work. The main achievement of the paper is that it incorporated different factors of insiders from their pre-

joining period to an organization until after they leave, to provide a comprehensive view of insider threat problems. Nevertheless, the paper did not consider the need to prevent infringement on employees' rights and dignity when monitoring employees' activities and behaviour in the work place. The paper also did not deal with the latest insider mitigation techniques such as deep learning.

Boakye-Gyan (2021) proposed six best practices for organisations and cybersecurity professionals to follow to develop a program to protect against insider attacks. The paper identified the best practices as (i) Plan to create an insider threat program and a dedicated insider threat office, (ii) Get top management buy-in and senior leadership engagement, (iii) Create an insider threat incident-response plan and insider threat mitigation team, (iv) Employ insider behaviour pattern monitoring and detection strategies, (v) Develop and implement a mandatory security awareness and insider threat training and education program, and (vi) Audit and review of the established insider threat program. The paper leveraged user behaviour analytics tools to provide insight into user activities, behaviour, and user access monitoring. The main limitation of the paper is that the framework was not based on sound risk management approach. Additionally, the framework proposed an insider behaviour pattern monitoring but did not consider ethical implications of monitoring employees' activities and behaviours.

Alsowail & Al-Shehari (2022) proposed a classification model that categorised insider threats prevention approaches into two classes: biometric-based and asset-based. The author provided insightful classification of biometric-based insider threat prevention into physiological, behavioural and physical, while the asset-based approaches were classified into host, network and combined. The main contribution of the paper was the recommendation of different commercially monitoring and surveillance systems referred to as Insider Risk Management (IRM) solutions designed for insider threat detection and protection. Although the framework provided a wide range of insight into insider threat detection, the approach did not address how to deal with data and indicators coming from different digital assets like computers, network tools, servers, and so on which could cause a huge damage to business and reputation if they are allowed to be breached.

Nurse et al. (2014) employed an insider centric approach that was based on the need to identify the elements of the insider threat problem. Their approach consisted of four elements namely: insider attack catalyst, actor characteristics, attack characteristics and

enterprise characteristics. They provided a comprehensive approach of the insider threat because of its insider centric approach. They examined a variety of attacks since the actor (individual) elements were as disparate as they come. The major achievement of the paper was that it provided insightful information on insider threat detection and encouraged organizations to delve deeper in gaining an understanding of the environment (catalyst), the attack (system) and the organization. However, the framework focused too much on the actor and discounted the disclosure of the insider threat. It also tended to be reactive as it focused on exposing insider attacks acts after their occurrence rather than being proactive.

Haran (2016) proposed a framework for detecting and mitigating insider threats at an early stage to provide an opportunity to prevent such threats and build a safe and secure e-governance ecosystem. The achievement of the framework was that it provides eight steps namely: Asset Identification and Classification, Role Mapping and Access Control, Establish Baseline Config and Pattern, Activity Logging and Monitoring, Robust HR Practices, Impact of Social Networks, Periodic Training and Awareness as well as Periodic Audit and Review. Each step handled different tasks that contributed to the detection and mitigation of insider threats. Two of the key components of the framework that played a very vital role in the success of the insider threat mitigation program was the periodic training and awareness to all the personnel involved in the e-governance projects as well independent audit for periodic / surprise assessment and review of the implementation and adherence levels of the personnel. However, the approach was not based on sound risk management approach.

Clifton (2024) employed a framework that was based on five components. These components were risk acceptance and tolerance, operating environment limitations, employee profiling, proactive measures, and measurement of success. A key aspect of the framework was the recommendation to implement a risk register for security gaps in their organizations to improve their insider threat mitigation strategies. The key contribution of the approach was that that can be utilized by IT manager to detect and mitigate insider threats. Although employee profiling was a key component of the strategies utilized to detect and mitigate insider threats in the paper, the framework failed to consider ethical implications of monitoring employees' activities and behaviours.

Sauer (2022) provided a comprehensive evaluating of insider threat indicators and mitigation measures based on Delphi studies. The paper provided possible insider threat mitigation measures that organizations can chose from to develop their tailor-made insider threat mitigation policy. The approach was a cyclical process that is comprised of nine stages, namely: Recruitment, Organisational socialization, Observation, Investigation, Anticipation, Damage limitation, Reconstruction, Deliberation, and Termination. The key achievement of the paper was the recommendation of measures and practices that can detect and mitigate insider threats at different stages. The main limitation of the paper was that the implementation of the results was based on Delphi studies which could be a challenge in real life (Kozak & Lefremova, 2014). The practical usability of the theoretical framework needs to be further improved by verifying the result before application in practical terms.

Gamachchi & Boztas (2018) proposed a graph-based framework for malicious insider threat detection. The paper utilised a hybrid framework that was based on graphical analysis and anomaly detection approaches. The framework analysed heterogeneous data in isolating possible malicious users hiding behind others. The framework generated anomaly scores based on different input parameters for each user. However, the framework was based on limited parameters (e.g. login/logoff behaviour, removable media usage, web access pattern, and psychometric observation)

Inayat et al. (2024) did an extensive literature review of insider threat mitigation measures. The framework proposed a multi-tiered activity-monitoring model that integrates real-time monitoring with behavioural analysis and access control. It offered a robust framework for preventing insider attacks by classifying prevention strategies into distinct categories, including network, behaviour, anomaly, analysis, access, and intention-based methods. The categories were designed to address various aspects of insider threat mitigation. The main limitation of the paper was that though it provided an insightful categorisation of anomaly detection and provided a very wide range of information for each category, it failed to address employee privacy and trust when their activities are monitored in the work place even though it employed the use of UEBA.

Montelibano et al (2012) proposed a framework titled Insider Threat Security Reference Architecture (ITSRA), The framework utilized a multi-tiered approach consisting of four security layers, namely: Business, Information, Data, and Application.

The layers provided a holistic solution to insider threat. The paper provided an insightful categorisation of measures that can be applied at each layer. At each of the layer adequate controls were required in the three security fundamentals of authorised access, acceptable use, and continuous monitoring. Organisations were required to implement countermeasures at every level to tackle insider threats. The four levels were interdependent and none can function as a standalone layer because of the association of pointers and application of controls cuts across all four layers and forms the most important point of this approach for Insider Threat Security Reference Architecture (ITSRA). The main achievement of the ITSRA is that it took cognisance of best practices and standards by addressing issues pertaining human rights, privacy and legal issues during implementation of the framework. The framework, however, did not have an arrangement for detecting the social actions of users. The no show of the psychological status monitoring means that the framework was limited in anticipating potential threat from employees in the organization.

Subhani et al. (2021) provided exhaustive classification of insider threats that can exist within an organization and the best methods for countering them. It described comprehensive classification of insider types, motivation, methods used and level of insiders. The main achievement of the paper was exhaustive description of the threat detection methods as well as insider threat analysis. Main limitation of the approach was that the efficacy of the detection methods was not tested using a live dataset. Again, the paper focused on reviewing the concept of insider and insider threat detection.

Rakhi et al. (2025) provided exhaustive review of strategies and safeguards to detect and prevent insider attacks such as behavioural-based anomaly detection, privilege access management, artificial intelligence (AI) and machine learning (ML), context aware access control, intrusion detection systems, security awareness and training. The key contribution of the paper is that it described insider threat dangers and offered strategies for seeing, dodging and overcoming insider attacks. Although several insider threats detection and prevention techniques were described, the paper did not apply any of the techniques to real-life scenarios.

Chauhan (2024) identified and analysed insider threats and its types. It evaluated detection techniques and examined prevention strategies. The key contribution of the paper was that it addressed the privacy and ethical concerns when detecting insider threats

as well as proposed integrated solutions that that combines technological solutions, organizational policies, and employee education to effectively manage insider threats. The ultimate goal is to provide actionable insights and recommendations that help organizations better detect, prevent, and respond to insider threats, thereby safeguarding sensitive information and maintaining system integrity. The main limitation of the paper was that it did not explore application of emerging technologies, such as artificial intelligence and blockchain, in insider threat management. Additionally, the impact of monitoring on employee privacy and the development of ethical surveillance frameworks was not explored to balance and effective approach to insider threat detection and prevention.

Pureti (2022) explored the nature and dynamics of insider threats, identifying key risk factors, motivations, and behaviours associated with internal security breaches. It highlighted effective strategies and technologies for detecting and preventing insider threats. The main contribution was that it advocated the importance of fostering a security-aware culture, implementing robust access controls, and leveraging advanced analytical tools to monitor and mitigate risks. However, there were potential biases in self-reported data from interviews and the reliance on publicly available datasets, which may not capture all insider threat incidents.

Max Alexander (2018) in the author's contribution explored insider threat by defining the problem and examining what makes an insider threat. The paper presented strategies to mitigate the threats posed by insiders. It identified mitigation strategies in terms of people, processes and technologies, and how each of these pillars can be used to protect, detect and correct insider threat activities and ultimately safeguard an organization's information. Although the paper identified certain controls administrators could use to protect data in all of their states and restore normal operations; to minimising the impact of the incident through corrective actions, the paper did not apply same to real-life incidents.

In his own contribution, Abuli (2016) examined different frameworks for dealing with insider threat problem in Kenyan public institutions. The main achievement of the paper was the recommendation for organisations to customise their mitigation strategies according to their peculiar goals. The study was limited to mitigation efforts by Kenyan parastatals and did not cover private institutions.

Gelles (2016) outlined a step-by-step path for developing an insider threat program within any organization, focusing on management and employee engagement, as well as ethical, legal, and privacy concerns. The paper provided valuable and in-depth explanation for mitigating supply chain risk. It outlined progressive approaches to cyber security. However, the paper did not apply any of the techniques to real-life scenarios.

In a paper titled Identifying and preventing insider threats, Waters (2016) examined different characteristics and behaviours that insider threats exhibit in the workplace. The main contribution of the paper was the identification of certain characteristics, behaviours, and motivations that separate insiders from rest of the company's employees. Another achievement was the conduct of research on the effectiveness of the preventive measures some of which were found to be efficient in preventing insider threats. The main limitation of the paper was that the research was based on limited preventative means of securing against insider threats. Another limitation was that security solutions are not one size fit all, the peculiarity of each environment in applying the controls was not taken into consideration.

The International Organization for Standardization (ISO) is another framework, like the NIST standards, that has a set of requirements for organizations to secure and protect their information systems (Dorrington, 2018). The ISO 27000 series was developed by the International Organization for Standardization. It is a flexible information security framework that can be applied to all types and sizes of organisations. The two primary standards - ISO 27001 and 27002 - establish the requirements and procedures for creating an information security management system (ISMS). While ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS, ISO/IEC 27002 provides a reference set of generic information security controls and guidelines to implement the control measures. According to Dorrington (2018), ISO does not directly address insider threats, nevertheless, the framework can be employed as a baseline to manage the threats posed by insiders. Boakye-Gyan (2021) concluded that though there exist a number of guidelines, standards and frameworks for managing cybersecurity, there was lack of a comprehensive framework to protect against insider attacks, whether intentional or unintentional.

Underlining Indicators of Insider Threats for a Proactive and Holistic Mitigation Strategy

To develop a holistic and proactive insider threat mitigation program, it is important to have a reflection on the underlining factors or indicators that could make an organisation vulnerable to insider attacks. Insider threat is getting increasingly sophisticated and diversified (Bedford, 2018). Having a clear understanding of indicators of insider threats from behavioural, organisisational or technical standpoint would go a long way to appreciate the challenges faced by organisations and can serve as a guide to develop an all-encompassing insider threat mitigation program. Bedford (2018) in his research work asserted that there is a growing recognition of the multi-factorial contribution to insider threat. The researcher noted that organisations, and experts in security, risk management and insider threat, are coming to convergence on the need for a holistic appreciation of the threat. Given that insider threat involves multidimensional risk indicators, and is a multidisciplinary concern, it requires a holistic approach for effective identification and mitigation. Greitzer, et al. (2019) provided reasons why researchers ignore such indicators. The reasons as indicated by the authors include lack of information, technical barriers, lack of studies to scientifically validate the proposed associations between behavioural indicators and insider threat risk; as well as privacy/ethical concerns about monitoring behavioural or psychological risk factors.

Developing a formal knowledge representation was considered a creative way to defining relevant factors to capture the concept that can serve as input to a robust insider threat mitigation framework. Greitzer et al. (2019) developed a formal representation to allow the understanding of factors underlying insider threats. They sought to extend current insider threat ontology frameworks by incorporating sociotechnical constructs reflecting both individual/behavioural and organizational factors.

Technical Indicators

Technical indicators are typically associated with digital traces left by user activities, which can be difficult to identify with insider threats. Security teams can look for signals, including unusual data access patterns, abnormal network traffic, unusual system logon times, or large volumes of sensitive data in unexpected locations. Bedford (2018) reflected that studies have in the past focused on how the insider threat problem can be addressed by implementing technological solutions.

Although preventing insider threat is the ultimate aim of security practitioners; detection, analysis, and identification of misuse has dominated the research (Neumann, 2010). The study of insider threat from a technical standpoint can be difficult due to the fact that threat landscape spans an IT system's life cycle; through design, development, operation, support and decommissioning (Cyber Security Division, 2009). For example, publications on technological solutions cover denial of access, fraud detection technology, access control (Crampton & Huth, 2010; Cyber Security Division, 2009), decoys (Bowen et al., 2010), anomalous pattern detection (Gelles, 2016), automated detection (Alsowail & Al-Shehari, 2022), use of big data (Festa, 2012a), and data mining, profiling, monitoring and multilevel security (Cyber Security Division, 2009).

Whilst there is a heavy emphasis on technological solutions to insider threat, a shift in focus has occurred over the past few years. For example, there has been a move to cover the importance of information security management (ISO 27001:2022 standard) and policy. Recently there has been a visible shift to integrate human aspects along with technological considerations. Computer technology on its own is not enough to combat insider threat and high level of computer sophistication is not necessarily a risk factor (Mouton et al., 2016). Cappelli et al. (2012) discovered through their research on insider threat that IT sabotage requires a level of technical sophistication and was often carried out by those in IT roles (e.g. system administration, database administration, programmers).

However, other insider crimes did not necessarily require high level technology skills. For insider theft of intellectual property, scientists, engineers, and sales people are amongst the highest offenders. In the case of fraud, lower-level employees in a variety of roles (and presumably with a variety of IT skill) are the biggest offenders. Insider threats are not technically sophisticated and often exploit business processes and policies (organisational level factors) rather than technical vulnerabilities (Randazzo et al., 2005)

There is a growing acknowledgement in cyber security research that personal predispositions contribute to an increase in risk and observable behaviours in the workplace can represent concern. Cappelli et al. (2012) identified in their research personal predispositions as: conflict with co-workers; bullying and intimidation; personality conflicts; unprofessional behaviour; inability to conform to rules; anger management concerns; and disgruntlement. Hence, combining psychosocial data along with the more traditional cyber security audit data may enhance the predictive capabilities of models of insider threat

(Greitzer, 2019). Whilst the emphasis beyond technological vulnerability and countermeasures is growing, limited research reflects a more holistic approach to insider threat with respect to psychosocial and organisational risks (Frangopoulos et al., 2013).

Greitzer (2019) agreed that a focus on cyber security and information technology alone does not provide a balanced solution, overlooking important individual and organisational interventions. Whilst security can be improved by technological assistance and advancement (e.g. passwords, data analytics, and multi-factor authentication) it does not address the full spectrum of insider threat. Employers can become comfortable and perhaps overly reliant on technology, missing the opportunity to embrace other proactive forms of addressing the insider threat (e.g. security awareness programs and personality testing). This is probably why surveys across industry consistently find that insider threat programs often lack direct focus on the suspicious non-technical behaviours of insiders (Intelligence and National Security Alliance, 2013).

Assessing insider threat requires a focus on technological, behavioural and organisational components. Greitzer (2019) emphasised on the importance of looking at the interplay between technology and overall business processes to ensure a comprehensive approach to insider threat. Gelles (2016) concured that policy, processes, communications, and training are critically important aspects of evaluating an insider threat program. Human factors, education and awareness, and after care are amongst the top priorities of consideration in the research effort (Greitzer, 2019). Furthermore, Bedford (2018) noted that while research in insider threat has increased, it has largely ignored the existing body of literature available on workplace deviance, especially as it relates to information and communication technologies (that is, cyber deviance). The author argued that placing pressure or demand on workers can cause discomfort or stress could potentially result in negative workplace behaviour

It is the combination of technical controls along with psychosocial considerations and organisational factors, that hold the most promise for understanding, detecting, and preventing insider threat (Gelles, 2016). A variety of disciplines contribute to the study of computer and information security (CIS). While individual and organisational factors have been a focus, further research is still an important consideration in extending knowledge and understanding of the interplay between individual, organisational, and information security (Safa et al., 2018). The author noted that streams of research have included

usability and users' role, user perceptions and behaviours, organisational policies, security culture, management support, employee training and awareness. Their specific study also expanded to include lack of funding, inadequate staffing, lack of CIS knowledge, and lack of CIS policies, among others, as contributing to security vulnerability, which is a precursor to insider threat.

Maasberg (2015) in his research study identified certain known insider espionage technical actions and indicators. The researchers proposed an espionage ritual model, derived by abstracting technical indicators to a higher-level cycle of technical objectives. This abstraction then allows for a more generalizable model, from which more robust technical detection mechanisms can be derived. The model suggested that the ritual is different for other insider threats, including sabotage, fraud and IP theft. Their research disclosed several significant commonalities and differences between cases. Some observables actions of insiders that signify technical indicators of insider threats are shown in Table 4.

Kauh et al. (2017) developed an indicator-based behaviour ontology (IB2O) for detecting insider threats in network systems. The model allowed the researchers to understand and interpret insiders' data packets, and then to detect potential threats in early stage in network systems including social networks and company networks. The researchers developed a model called Insider Threat Detecting Extractor (ITDE) for detecting potential insider threats in early stage based on the behaviour ontology. Insider threat behaviour for data leakage was classified in higher level, and then investigate relationship between the behaviour and network packets with protocols used in data leakage on the Internet as well as local network. Employees behaviours which could become insider threat were divided into five classifications (print, search, access, download and browse). Warning signs of insider threats were defined such as evasiveness, suspiciousness, and anomalies regarding each activity. To show the practicality of the proposed ontology, the researcher developed ITDE which can collect network packets from network systems, and also detecting insider threat behaviours based on the IB2O regarding the collected network packets. With the ITDE, they performed evaluation using CERT data. They were able to show that the IB2O can detect insider threat behaviours using network packets and concluded with confidence that the IB2O can eventually contribute to detecting insider threat behaviours in network systems.

Organisational Indicators

Organisational factors have been identified in a large body of research from industrial/organizational psychology and human factors research on human errors, including communication issues, work setting/management systems, work planning, control, security practices and cultural orientation (Greitzer et al., 2019). This holistic approach enhances threat detection by recognizing insider threats, often involving technological misuse and human factors. The importance of these indicators lies in their ability to highlight anomalies that enable early detection and prevention of insider threats.

Shaw & Sellers (2015) acknowledged that organisational and situational factors can contribute to insider threat. The way companies recruit, train and manage staff are important considerations when looking at overall organisational security given that effective management can reduce risk and strengthen controls (Shaw & Sellers, 2015). Similarly, organisational culture, working conditions and pressures on organisations can also be relevant considerations when it comes to insider threat (Tang et al., 2016),

Research by the Centre for Protection of National Infrastructure (CPNI, 2013, p. 5) in the UK noted that organisational level factors are exploited in insider cases and that vulnerability to insider threat may be reduced by identifying organisational level factors and ensuring "a strong, on-going personnel security regime, establishing effective management practices and recognising that the insider threat can come from anyone with access to an organisation's assets".

It is important to note that organisations can place demands on their workers that can cause discomfort or stress and therefore could potentially result in negative workplace behaviour. Research in employee behaviour and occupational health has consistently shown that, among others, restructuring, temporary work conditions, job insecurity, high workloads and working hours, poor workplace relationships, poor working conditions, and lack of work-life balance can all contribute to greater stress in individuals (Bedford, 2018)

It was established that organisation specific sources of risk can escalate insider threat behaviour. An organisations response to its staff may increase or decrease the likelihood of insider threat and make matters worse through some action or failure to act (Shaw & Sellers, 2015). A variety of studies have found that a high workload can affect security behaviour. In addition, globalisation (including inter-company collaboration) and the internet have contributed to an increase in insider threat (Bedford, 2018).

Reports on unethical behaviour in organisations is increasing with informal norms contributing to negative employee behaviour (Shaw & Sellers, 2015). Research found that organisational environments can influence employee expectations. For example, organisations which ignore stealing can set an expectation that this behaviour is socially acceptable. Vashisth & Kumar (2013) wrote in their article about the 'Bad Barrel' approach, which hypothesises that unethical behaviour (such as insider threat) is more a function of organisational and societal factors. As such it is assumed organisational factors strongly influence insider threat behaviour (including leadership, policy and process and culture) and that some organisational environments will encourage insider threat activity (Vashisth & Kumar, 2013). Further, the behaviour of leaders and their ability to model sound security practices may assist in developing a positive security culture.

The employment of specific types of employees, such as hackers, may also have important implications for organisational culture. Whilst organisational factors are a strong consideration, creating opportunity, an individual's characteristics and social networks cannot be overlooked (Vashisth & Kumar, 2013).

Behavioural Indicators

Individual or behavioural indicators apply to the human element of the detection equation. Human elements significantly contribute to the complexity of insider threats. Insider threats are often precipitated by changes in behaviour, which can serve as early warning signs of a potential issue. Bedford (2018) used Delphi method through consensus to arrive at human factors that increase the risk of intentional insider threat. Behavioural factors can be considered from demographic, motivational or psychological perspectives (Bedford, 2018). Each of these characteristics is considered in the following sections:

(a.) Demographic Indicators

Demographic approaches to the study of insider threat look at historical cases in order to identify common characteristics or traits of the perpetrator. Earlier research into insider threat, used this approach to draw statistical conclusions about the common demographical characteristics across espionage cases (Bedford, 2018).

(b.) Motivational Indicators

Motivation is defined in the online Oxford Dictionary as 'a reason or reasons for acting or behaving in a particular way'. Shaw & Sellers (2015) noted that individuals

participating in negative insider behaviours are 'frequently driven by the same motivations – greed, disgruntlement, conflicting loyalties, and ego-satisfaction'. Such motivations are consistently reported in other writings as well (Vashisth & Kumar, 2013).

Research elaborates that motivation differs based on the type of insider crime. For example, Cappelli et al. (2012) report, based on large scale research, that IT sabotage is usually motivated by revenge whilst insider fraud is motivated by financial need or greed. It is also argued that money is a larger motivation in volunteer spies and those recruited by foreign intelligence, but ingratiation is more evident in those recruited by family or friends.

Sokolowski et al. (2015), suggested that as a generalisation, motive is associated with some type of "gain"; financial gain, competitive advantage, and/or retaliation. Research on insider threat focusing on individual motivations has included loyalty and allegiance and response to boredom, professional setbacks or unmet expectations (Shaw & Sellers, 2015), as well as an interest in hacking. Research has indicated that individuals may not be motivated by their work environment or by the purpose of the organisations in which they work. Additionally, professional setbacks or unmet expectations are highlighted as having the potential to accelerate an individual from intent to action (Shaw & Sellers, 2015).

(c.) Phycological Indicators

A large portion of research focused on individual characteristics that may lead to insider threat behaviour and for a number of researchers the main aim is to identify psychological predispositions which can indicate higher potential to participate in insider threat activity (Bedford, 2018). Research has continued to demonstrate similar findings and expand our understanding of psychological predispositions that are linked to insider threat (Bedford, 2018). Personality vulnerabilities identified in the research includes psychopathy, malignant narcissism, and borderline personality organisation (Liang & Biros 2016), as well as personal predispositions such as medical or psychiatric disorders that affect judgment and social skill problems (Shaw & Sellers, 2015). Bedford (2018) identified that disgruntlement, anger management, disengagement and disregard for authority as important tendencies toward insider threat.

Further ethical flexibility, entitlement, and lack of empathy are also identified as personal predispositions that can trigger insider threat. More recently in a proof-of-concept study, Liang & Biros (2016) presented more positive individual characteristics associated

with insider threat. Acknowledging the limitations of a pilot study (including a small test set of cases and related low power) Liang & Biros (2016) discovered that cognitive ability, dedication, and being well-educated, were characteristics of their group of cases.

When it comes to insider threat, much of the research notes that psychological and personality predispositions are not enough on their own. It is the interaction of the vulnerability, with a current stressor, which can lead to poor judgment, especially where no social support is available for effective intervention (Bedford, 2018). This is an important consideration given the prevalence of exposure to psychosocial risks by the workforce. Surveys and research indicate that as much as one third of the workforce is exposed to psychosocial risks and therefore "could conceivably pose a significant threat to the enterprise's prosperity" (Frangopoulos et al., 2013, p. 55).

Previous research on psychological and organizational aspects of insider attack had suggested that insider attack is often preceded by behavioural indicators such as disgruntlement, gambling, organizational rule-breaking, organizational conflict, and behavioural deviance (Bedford, 2018). Financial stressors or psychological factors can motivate harmful actions, while personal and personnel security practices can mitigate or amplify the risk. Behavioural cues may range from observable disgruntlement or dissatisfaction, decreased productivity, and frequent conflicts with co-workers to more subtle signs, such as evidence of unexpected lavish lifestyle changes or individuals living beyond their means (Bedford, 2018). Other behaviours can include erratic attendance, changes in mood, substance abuse issues, and working unusual hours. Another frequent indicator is when individuals violate organizational IT and data management policies. By searching through industry best practices and frameworks, indicators of insider threats spanning technical, organisational and behavioural indicators that could signal potential insider attacks can be identified (Table 3).

Table 3: Technical, Organisational and Behavioural Indicators of Insider Threats Summary

Technical Indicators	Organisational Indicators	Behavioural Indicators
a.Access of information outside of need to know	a.Inadequate hiring practices	a.Medical or psychiatric disorders that affect judgement
b.Download and installation of malicious code and tools	b.Security training and awareness practices	b.Lack of individual coping mechanism

Technical Indicators	Organisational Indicators	Behavioural Indicators
c.Hacking or cracking activities	c.Policy clarity	c.Repeated unplanned time-offs
d.Unathorised encryption of information	d.Poor communication	d.Disgruntlement
e.Unauthorised information transfer	e.Inadequate Policies and Procedures	e.Anger Management
f.Violation of acceptable use policy	f.Non-Productive Work environment	f.Disengagement
g.Copying information on disks	g.Insufficient Resources	g.Disregard for Authority
h.Relabeling of disk	h.Lack of clear advancement	h.Ethical flexibility
i.Violation of physical security policies and procedures	i.Poor Management Styles	i.Criminal Record, Personal History, Ideology
j.Download and use of password cracker	j.Job instability	j.Interpersonal Problems
k.Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material	k.Restructuring, Temporary work conditions, High Workloads, Poor Working Conditions, Lack of Work-life Balance	k.Addiction (particularly gambling
l.Frequent visits to job portals or job hunting	l.Inadequate hiring practices	l.Affiliation (religious, criminal)
m.Lack of electronic access control	m.Lack of consistency of policies and expectations across all levels of the organisation	m.Social Engineering
n.Limited hardware controls	n.Lack of monitoring and enforcing policies	n.Security Policy Violation
o.Limited authentication procedures	o.Lack of oversight of senior managers	o.Erratic attendance, changes in mood, substance abuse issues, and working unusual hours
p.Lack of electronic access control	p.Perception that managers do not value staff	p.Malignant narcissism
q.No/limited auditing and monitoring	q.Complacency	q.Borderline personality

Technical Indicators	Organisational Indicators	Behavioural Indicators
r.Unathorised encryption of information	r.Lack of connection to employee issues	r.Personality vulnerability/disorder
s.Compromise of supervisor's computer	s.Lack of management of issues at the merging stages	s.Criminal association
t.Unathorised web surfing	t.Poor application of security	t.Disgruntlement
a.Unauthorized downloads or uploads of sensitive data	u.Poor organizational communication	u.Ego or sense of entitlement
a.Excessive printing of documents	v.Poor security practices of leadership	v.History of security violation
b.Unauthorised network access	w.Witnessing other staff get away with poor security behaviour with no consequence	w.Financial concern that could lead to embarrassment

Results and Discussion

The primary source of threats to information assets continues to be human users (Rakhi et al. (2015). The paper presents an overview of relevant frameworks and shows how they have limitations in one area or the other. It was observed that earlier work focused on limited scope of the measures required to identify and mitigate insider threats. For example, Rakhi et al. (2025) described insider threat dangers and offered strategies for seeing, dodging and overcoming insider attacks but none of the techniques were applied to real-life scenario. Pureti (2022) presented a framework for effective strategies and technologies for detecting and preventing insider threats but there were potential biases in self-reported data from interviews and the reliance on publicly available datasets, which may not capture all insider threat incidents. Similarly, Inayat et al (2024) proposed a framework for preventing insider attacks by classifying prevention strategies into distinct categories, including network-, behaviour-, anomaly-, analysis-, access-, and intention-based methods. The framework employed the use of UEBA but with limited concern for employee privacy and trust issues. Haran (2016) examined the role of training in mitigating insider threats; empirical evaluations of different training methods' effectiveness were limited. More studies are therefore needed to understand how various training approaches impact employee behaviour over time (Farnham, 2018). As technology evolves, so do the

methods and vectors of insider threats. Research is needed to assess how new technologies, such as cloud computing and remote work tools, change the landscape of insider threats and how frameworks can adapt accordingly (Liu, 2020). Other notable gaps identified in this review include reactive or one-size-fits-all control deployment, poor visibility into internal behaviour of employees, siloed cybersecurity and human resource policy efforts as well as delayed or ineffective responses. While organizational culture is acknowledged as a factor in some studies, empirical studies specifically linking cultural dimensions to insider threat behaviours were scarce. The gaps revealed here were corroborated by Boakye-Gyan (2021) with the claim that though there exist a number of guidelines, standards and frameworks for managing cybersecurity, there was lack of a comprehensive framework to protect against insider attacks, whether intentional or unintentional

To address all of these gaps, an integrated, layered and structured framework is recommended. This research provides a comprehensive overview of the current landscape of insider threat management, highlighting the critical need for enhanced predictive and preventive measures. Our findings suggest that future research should prioritise developing robust, adaptive solutions that integrate multiple methodologies to effectively mitigate insider threats.

Conclusion

This paper provides a comprehensive systematic literature review of insider threat examining different types of insiders and related incidents that have compromised organisations' security measures. The results highlight the potential risks to organisational security posed by both malicious and negligent insiders, and emphasise the importance of understanding underlining indicators of insider threats that will be useful when cybersecurity experts design solutions to identify and mitigate the risk of insider threats. This paper provides valuable contributions to the field of cybersecurity by identifying behavioural, organisational and technical factors that increase the risk of insider threats. The findings of this review emphasise the importance of utilising an integrated, structured and end-to-end approach that combine behavioual, organisational and technical controls to proactively identify and mitigate insider threats. It is recommended that future solutions contain a privacy preserving monitoring component to maintain employee buy-in and trust. Finaly, there is the need for security experts to leverage emerging technologies such as

artificial intelligence (AI), blockchain, data loss prevention (DLP), among others, when designing an insider threat detection and prevention systems in view of the expanding attack surface arising from widespread adoption of cloud computing, remote work, and bring-your-own-device (BYOD) policies.

References

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, Vol 4, No 1, pp 65-88.

Abuli, M. J. (2016). A Framework for Assessing the Insider Threat in Parastatals in Kenya (Doctoral dissertation, University of Nairobi).

Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. PeerJ Computer Science, DOI 10.7717/peerj-cs.938

Alsowail RA & Al-Shehari T. (2021). A multi-tiered framework for insider threat prevention. Electronics. 10(9):1005, pp 1-30, DOI 10.3390/electronics10091005.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber- harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1), Vol. 4, Issue 1, pp. 1 - 4.

Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences, 10(15), 5208, 1-41.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. Pp 1-42. https://doi.org/10.3390/electronics12061333

Balakrishnan, B. (2015). Insider threat mitigation guidance. Retrieved from: https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307.

Bedford, J. (2018). Organisational vulnerability to intentional insider threat. (Doctoral dissertation, University of Southern Queensland). https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Organisational+vulnerability+to+intentional+insider+threat&btnG= Accessed 24 July, 2024.

Boakye-Gyan, K. (2021). An Approach to a Comprehensive Framework for Insider Threat (Doctoral dissertation, Capitol Technology University).

Bilusich, D. A. N. I. E. L., Chim, L. E. U. N. G., Nunes-Vaz, R. A., & Lord, S. (2018). There is no single solution to the 'insider'problem but there is a valuable way forward. WIT Transactions on Engineering Sciences, 121, 135-146.

Cappelli DM, Moore AP & Trzeciak RF (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). https://scholar.google.com/scholar?q=The+CERT+guide+to+insider+threats:+h

ow+to++prevent,+detect,+and+respond+to+information+technology+crimes+(theft,+sabotage,+fraud).&hl=en&as_sdt=0,5.

Chauhan, K. (2024). Insider Threats Mitigation: Role of Penetration Testing. arXiv preprintarXiv:2407.17346. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Insider+Threats+Mitigation%3A+Role+of+Penetration+Testing&btnG=. Accessed June 26, 2025.

Clea Ostendorf (2023), 11 Real-Life Insider Threat Examples, https://www.code42.com/blog/insider-threat-examples-in-real-life/ assessed on May 20, 2024

Clifton, A. (2024). Strategies for Insider Threat Mitigation and Detection (Doctoral dissertation, Walden University).

Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. Scandinavian Actuarial Journal, *2023*(10), 1000-1021. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Managing+cyber+risk%2C+a+science+in+the+making&btnG=.

Dorrington, M. (2018). Future insider threats: A Delphi analysis (Doctoral dissertation). Available from ProQuest (Accession No. 13427366).

Farnham, S. D. (2018). "Evaluating the Impact of Security Training on Employee Behaviour." Information Systems Security, 27(2), 175-186.

Frangopoulos, ED, Eloff, MM & Venter, LM (2013). 'Psychosocial risks: can their effects on the security of information systems really be ignored?', Information Management and Computer Security, Vol. 21, No. 1, pp. 53-65.

Gamachchi, A., Sun, L., & Boztas, S. (2018). A graph-based framework for malicious insider threat detection. arXiv preprint arXiv:1809.00141. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=A+Graph+Based+Framework+for+Malicious+Insider+Threat+Detection&btnG=, accessed on May 15, 2025.

Gelles, MG (2016). Insider Threat: Prevention, Detection, Mitigation, and Deterrence, Butterworth-Heinemann, US. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Insider+Threat%3A+Prevention%2C+Detection%2C+Mitigation%2C+and+Deterrence&btnG=. Accessed August 15, 2024.

Global cybersecurity outlook (2022) insight report,https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022. Accessed on June 24, 2024.

Greitzer, F. L. (2019). Insider threats: It's the HUMAN, stupid! NCS '19: Proceedings of the Northwest Cybersecurity Symposium, 1–8. doi:10.1145/3332448.3332458

Haran, M. H. (2016). Framework Based Approach for the Mitigation of Insider Threats in E-governance IT Infrastructure. *International Journal of Scientific Research*, *3*(4), 5-10.

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing, 44, 655-662.

Holger, S. (2023). Insider Threat Report, https://nationalcioreview.com/wp-content/uploads/2024/07/2023_Insider_Threat_Report-16d8d8f7.pdf, accessed on June 15, 2024.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 1-40.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, pp. 3171-3189.

Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal*, 103068. Accessed on May 15, 2025.

Kauh, J., Lim, W., Kwon, K., Lee, J. E., Kim, J. J., Ryu, M., & Cha, S. H. (2017). Indicator-based behaviour ontology for detecting insider threats in network systems. KSII Transactions on Internet and Information Systems (TIIS), 11(10), 5062-5079.

Liang, NP & Biros, D (2016). 'Validating common characteristics of malicious insiders: Proof of concept study', 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, pp. 3716-3726.

Liu, L.; De Vel, O.; Han, Q.-L.; Zhang, J. & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Commun. Surv. Tutor. 1397–1417.

Liu, J. (2020). "The Impact of Cloud Computing on Insider Threats: A Comprehensive Review." Future Generation Computer Systems, 108, 146-155.

Maasberg, M. (2017). An empirical examination of insider threat revenge behaviours for analyzing high risk insiders exhibiting subclinical psychopathic traits (Doctoral dissertation. Retrieved from ProQuest Dissertations and Theses Global. (1906305261)).

Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: detecting the insider threat through examination of dark triad personality traits. In 2015 48th

Max Alexander, C. I. S. M., & CRISC, C. (2018). Protect, Detect and Correct Methodology to Mitigate Incidents: Insider Threats. https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/protect-detect-and-correct-methodology-to-mitigate-incidents-insider-threats. Accessed June 28, 2025.

Modini, J., Vanzomeren, M., Fowler, S., Joiner, K., & Lynar, T. (2020). Rising to the Challenge of Insider Threats for Middle Powers. Academic Conferences International Limited. 92 http://dx.doi.org/10.34190/ICCWS.20.131

Morrow, S. (2020). 8 of the world's biggest insider threat security incidents. Retrieved January 22, 2021, from Infosec Resource https://resources.infosecinstitute.com/topic/8-of-the-worlds-biggest-insider-threatsecurity-incidents/

Mouton, F, Leenen, L & Venter, HS (2016). 'Social engineering attack examples, templates and scenarios', Computers and Security, Vol. 59, pp. 186-209.

Neumann, P. G. (2010). Combatting insider threats. In Insider Threats in Cyber Security (pp. 17-44). Boston, MA: Springer US.

Nurse, J. R. C., Buckley, O., Legg, P., Goldsmith, M., Creese, S., Wright G. & Whitty, M. (2014). *Understanding insider threat: A framework for characterizing attacks*. Retrieved from https://www.cs.ox.ac.uk/files/6576/writ2014_nurse_et_al.PDF.

Ponemon Cost of Insider Threats Global report, (2022). Viewed 26 July 2024). https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

Pureti, N. (2022). Insider Threats: Identifying and Preventing Internal Security Risks. International Journal of Advanced Engineering Technologies and Innovations, 1(2), pp.98-132.

Rakhi, S., Sampada, H. K., Balodi, A., Shobha, P. C., & Kumar, R. (2025). Insider Threat Detection and Prevention: New Approaches and Tools. Emerging Threats and Countermeasures in Cybersecurity, 241-262.

Rama K. (2023). The Different Types of Insider Threats and How to Stop Them. https://www.google.com/url?sa=tandsource=webandrct=jandopi=89978449andurl=https://www.securonix.com/blog/stop-insider-threats. Viewed 31 August, 2024.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460.

Safa, NS, Maple, C, Watson, T & Von Solms, R (2018). 'Motivation and opportunity-based Model to reduce information security insider threats in organisations', Journal of Information Security and Applications, 40 (2018): pp. 247-257.

Shaw, ED & Sellers, L (2015). 'Application of the critical-path method to evaluate insider risks', Studies in Intelligence, vol. 59, no. 2, pp. 1-8, viewed 01 September 2015, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Shaw-Critical%20Path-June-2015.pdf>

Singleton, C. (2021). X-force threat intelligence index (Tech. Rep.). Armonk, NY: IBM. https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report-gurucul/

Sokolowski, J & Banks, C (2015). 'Agent implementation for modeling insider threat', Winter Simulation Conference (WSC), 06-09 December 2015, Huntington Beach, CA, USA, pp. 266-275.

Subhani, A., Khan, I. A., & Zubair, A. (2021). Review of insider and insider threat detection in the organizations. Journal of Advanced Research in Social Sciences and Humanities, 6(4), 167-174.

Tang, M, Li, Mg & Zhang, T (2016). 'The impacts of organizational culture on information security culture: a case study', Information Technology and Management, Vol. 17, No. 2, pp. 179-186.

Tessian. (2021). The psychology of human error - tessian (Tech. Rep.). Broadgate Circle, UK:https://www.code42.com/blog/insider-threat-examples-in-real-life/

Tongkaw, A. (2019). Software defined network, the design, technique, and internet of things defined in campus network. International Journal of Technology and Engineering Studies, 5(3), 80–89. doi:https: //dx.doi.org/10.20469/ijtes.5.10002-3.

Vashisth, A and Kumar, A (2013). 'Corporate espionage: the insider threat', Business Information Review, Vol. 30, No. 2, pp. 83-90.

Waters, M. D. (2016). Identifying and preventing insider threats. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Identifying+and+Preventing+Insider+Threats&btnG=. Accessed June 28, 2025.