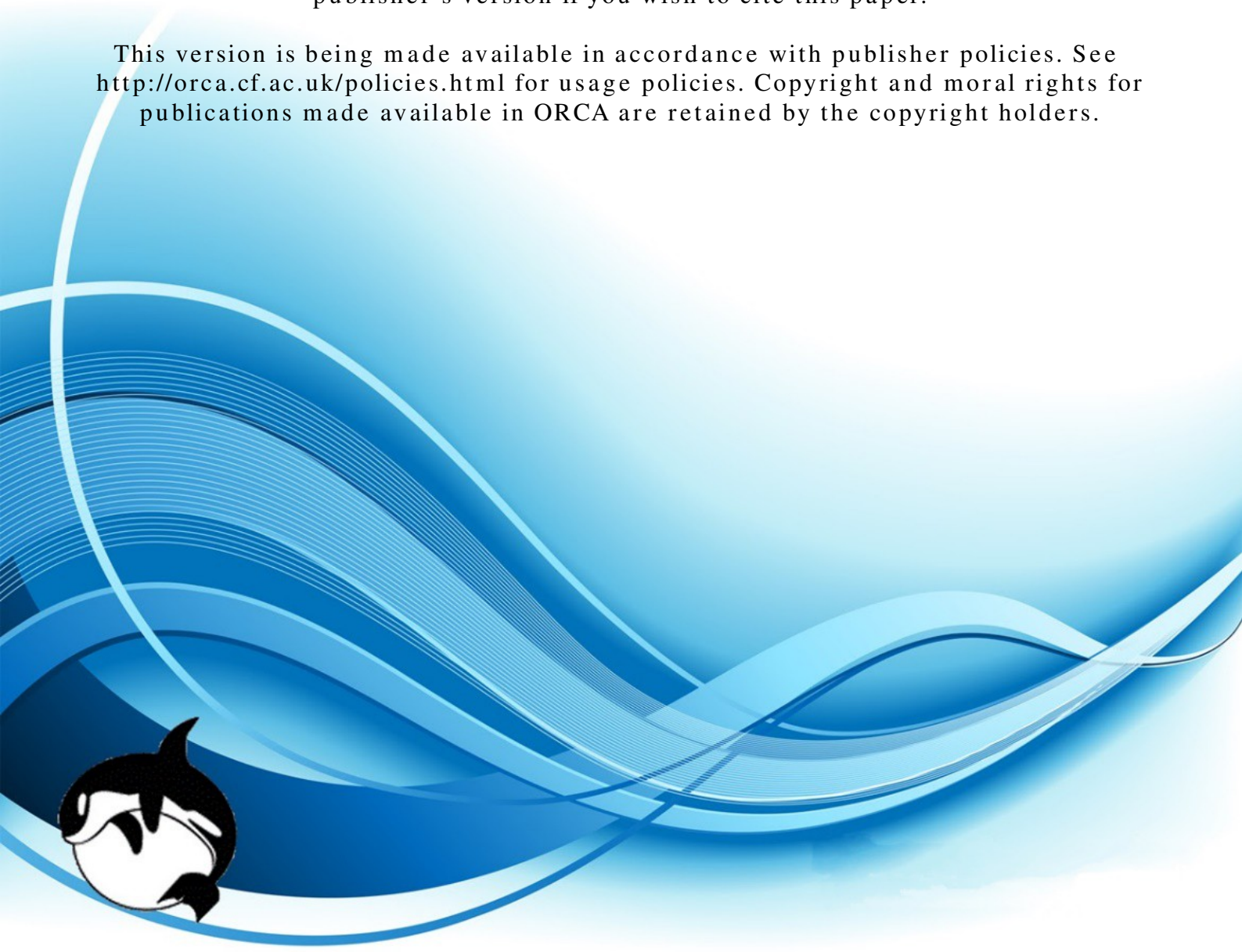

electronics

MDPI

Review

Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses

Neetesh Saxena [1,*], Emma Hayes [2], Elisa Bertino [3], Patrick Ojo [2], Kim-Kwang Raymond Choo [4] and Pete Burnap [1]

[1] School of Computer Science and Informatics, Cardiff University, Cardiff CF10 3AT, UK; burnapp@cardiff.ac.uk
[2] Department of Computing and Informatics, Bournemouth University, Bournemouth BH12 5BB, UK; i7711991@bournemouth.ac.uk (E.H.); s5119590@bournemouth.ac.uk (P.O.)
[3] Department of Computer Sciences, Purdue University, West Lafayette, IN 47907, USA; bertino@purdue.edu
[4] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA; raymond.choo@fulbrightmail.org
* Correspondence: nsaxena@ieee.org

Received: 29 July 2020; Accepted: 27 August 2020; Published: date

Abstract: The insider threat has consistently been identified as a key threat to organizations and governments. Understanding the nature of insider threats and the related threat landscape can help in forming mitigation strategies, including non-technical means. In this paper, we survey and highlight challenges associated with the identification and detection of insider threats in both public and private sector organizations, especially those part of a nation's critical infrastructure. We explore the utility of the cyber kill chain to understand insider threats, as well as understanding the underpinning human behavior and psychological factors. The existing defense techniques are discussed and critically analyzed, and improvements are suggested, in line with the current state-of-the-art cyber security requirements. Finally, open problems related to the insider threat are identified and future research directions are discussed.

Keywords: cyber kill chain; insider threat; attack vectors.

1. Introduction

The threats that insiders pose to government organizations, businesses, and institutions continue to be a critical concern. Current research provides unambiguous evidence that emphasizes the severity and prevalence of this threat in businesses today [1], [2]. According to a 2020 global report [3], the average global cost of insider threats rose by 31% in the last two years to $11.45 million, and the occurrence of incidents spiked by 47% in that period. Through the assessment and analysis of incidents, the challenge of insider threat (IT) can be better understood and addressed. For example, the Threat Landscape Report 2016 [4] by the European Union Agency for Cybersecurity (ENISA) classified the top four insider incidents/actions as follows: privilege abuse (60%), data mishandling (13%), use of non-approved hardware (10%), and abuse of privilege possession (10%). As per the Threat Landscape Report 2018 [5] by the ENISA, 27% of data breach incidents were caused by human factors or negligence and according to a study, phishing (67%) is the major issue in the case of unintentional insider threats. Weak or reused passwords (56%), unlocked devices (44%), password sharing practice (44%), and unsecured Wi-Fi networks (32%) were also part of the list of unintentional insider threats. Moreover, the report identifies that the prevalence of these attacks has increased to 56%, whilst 30% of organizations believe that they have experienced one too many attacks. Therefore, this enunciates the crucial need for preliminary defensive actions to be executed by organizations to combat this threat.

Typically, businesses invest in security defenses to strengthen their network against outside malicious attacks. However, they fail to deploy protection against potential threats by malicious or compromised insiders. Insiders can abuse their authorized access to critical systems and eventually steal or modify data systems for malicious intent or financial gain [1]. Insider threat targets not only private sector enterprises, but also government institutions and critical infrastructures for motives, ranging from monetary gains and industrial espionage to business advantage and sabotage [2]. Because insiders have access to valuable information assets that are unavailable to outsiders, damages resulting from insider attacks can be devastating. Furthermore, these threats are increasing in scale, scope, and sophistication; thus, emphasizing the critical need for organizations to apply current security techniques.

According to the Centre for the Protection of National Infrastructure (CPNI) [6], an insider is someone who exploits or has the intention to exploit their legitimate access to an organization's assets for unauthorized purposes. Furthermore, credentials are provided to trusted employees, such as username and passwords, therefore offering a gateway to an organization's information network, meaning concealment within the infrastructure is effortless [7]. This threat is sophisticated enough to compromise the security principles of confidentiality, integrity, and availability that must be guaranteed for any secure defense system [8]. As per a recent survey, 27% of the total cyber crime incidents were supposed to be conducted by insiders, and 30% of respondents specified that the destruction caused by insiders was more severe than the loss caused by external attackers [9].

1.1. Context and Scope

ENISA [4] has demonstrated the dangers of the insider threat for the security of organizations, epitomizing the critical need to address them. The present work aims to extend the knowledge of how insider threat is expanding and to detail the comprehensive actions required by organizations to address the critical risks it poses. This is imperative as organizations are constantly directing funding into traditional strategies that are unable to protect against the insider threat. This paper introduces how the technologies/tools used by insiders can expand through all seven stages of the kill chain that are recognized in many cyber-attacks. From the tools that insiders use, the present work proposes a layered defense approach involving policies, organizational culture, and technical environment to combat the threat.

1.2. Our Contribution

To protect critical assets, organizations must recognize the nuances and breadth of this threat. This paper endeavors to provide an informed evaluation of the insider threat that is perpetual and destructive for organizations everywhere. The technologies and practices insiders use are identified with explained relevance to the cyber kill chain. The practices that organizations should use for defending against insider threats are highlighted with common best practices and recommendations to assist in combating the threat. Concluding, a critical evaluation of the respective threat is presented, from understanding the nature of the threat to the best security defenses with the current state of the art research.

A survey in [10] presents data of 105 enterprise users that reveal the insider threat emerging from trusted employees and inconsistent practices. However, the work does not highlight any detection or remedial methods to combat insider threats. Further, a survey study in [11] considered only the three most common types of insider threats: traitor, masquerader, and unintentional perpetrator, and discussed their countermeasures from a data analytics perspective. The work [12] presents a detailed survey on insider threats that decently summarizes the structural taxonomy of insider threat incidents. Their approach, however, focused on the relevant dataset and the other aspects of the insider incidents and their countermeasures. Open issues and future directions are only partially discussed. The work [13] conducted a systematic review of 37 articles from the period 1950–2015. It analyzed best-to-date insider threat detection and prediction algorithms and then ranked them, but excluded theoretical papers. Our study presents a novel aspect of the insider threats as to

their significance to the cyber kill chain. Hence, our work compliments the existing survey works on the insider threat. Now, we summarize our three-fold contribution as follows:

1. As a novel contribution to the literature, we identified the relevance of insider threat to the cyber kill chain and its propagation through different phases.
2. We evaluated the current state of the art (threat landscape) in terms of understanding the nature of insider threat, assessing associated risks, highlighting the effectiveness of techniques in detecting and mitigating risks, and propose enhancements for mitigating the impact of such threats.
3. We highlighted open problems and future directions for addressing insider threats in different forms targeting several subsystems of the organization.

1.3. Paper Organization

The rest of the paper is organized as follows. Section 2 provides an understanding of the nature of the insider threat, including different goals and types of insiders. Section 3 discusses the potential attack vectors (e.g., technologies, tools, and practices). Section 4 uses the cyber kill chain to understand an insider attacker. Sections 5 discusses various mitigation strategies and their evaluation, respectively. Finally, Section 6 concludes this work and highlights future directions.

2. Understanding the Nature of Insider Threats

The nature of insider threat needs to be explored to enhance the understanding of insider threat. Therefore, the many different types of insider threats need to be distinguished. Definitions vary from the misuse of privilege abuse to broader definitions involving the effect on the confidentiality, integrity, and availability of corporate data [14]. The substance of these definitions depicts trusted personnel abusing their privileges for specific purposes to cause detrimental effects to a corporation.

2.1. Types of Insiders

Abnormal activities could be an indication of the inside threat. A few examples could be an activity at unusual times (e.g., logging into the system late at night), a large volume of data traffic (e.g., transmitting too much data over the network), and unusual or not routine activity (e.g., accessing unusual machine or database). Generally, these activities are resulted in when the employees appear not to be satisfied with the system or employer. Here, we consider mainly three types of insiders: malicious insider, compromised insider, and careless insider.

Malicious insider: An insider who intentionally abuses legitimate credentials maliciously to steal information for financial or personal gains [15]. For example, an individual who dislikes the employer can sell secret information to an outsider. They could be a great benefit to the competitors as these insiders generally do have sufficient knowledge about the security policies and practices as well as the vulnerabilities of the organization.

Compromised insider: An insider whose account credential has been harvested and unintentionally enables an attacker to access sensitive information or resources [16]. For example, an attacker can target a compromised insider by harvesting his login credentials through social engineering and then accesses confidential assets, which can result in the theft of an organization's intellectual property (IP) or other personably identifiable information (PII). Social engineering is a technique representing malicious activities that are targeted through human interactions to either inject a malware or retrieve sensitive information. It applies psychological manipulation to trap users making security mistakes or overlook associated risks. Detecting such an attack is quite difficult, as the attacker uses the legitimate credentials of an authorized user, which will generally not trigger any security alerts.

Careless insider: This category of the insiders includes people who make the most common mistakes and generally do not pay significant attention to the security practices of the organization. An insider under this category unintentionally and unknowingly exposes the key resources to the outsiders. For example, a receptionist employee who does not realize the security threat to the system

can click on the insecure links, which may enable outsiders to get access to the system or key resources.

For the first two types, typically the attacker carries out attacks differently, whereas, for the third one, there will not be any deliberate attacks.

2.2. Goals for Insider Attacks

Typically, the objectives of insider fraud can range from theft of information assets and direct theft of the corporation's funds to trading data for personal gain [17]. Four types of insider threats have been established through the motive and purpose of an attack: fraud, sabotage of infrastructure, theft of IP, and unintentional insider threat (UIT) [18].

Insider fraud: This has been regarded as one of the most common forms of attack, with 61% of companies rating it extremely prevalent within their corporation [17]. Most of the time, the intention of the insider leading a fraud is financial gain. This emphasizes the clear need for organizations to develop mitigation measures to protect assets as financial gain is an influence in these attacks.

Insider threat sabotage: It is committed typically by insiders with technical positions and highly sophisticated skills. They involve privilege escalation techniques and the implementation of malware such as advanced persistent threats (APTs) to disrupt information systems. The motives behind these attacks are harming the organization's data or a specific individual due to disgruntlement, unmet expectations, or stress [19].

IP Theft: IP theft involves stealing crucial data, including source code or customer information. Attackers use technical strategies like phishing emails or network transfers who have legitimate access. Kaspersky [10] found that 75% of the data that were stolen from organizations, the user had authorized access to. However, there are still high statistics that insiders with no legitimate access using the same techniques are still damaging the organization's assets.

Unintentional Insider: The Community Emergency Response Team (CERT)'s insider threat team (a part of the Carnegie Mellon University's Software Engineering Institute) uses the following working definition of UIT [20]:

"An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems".

The rise in UIT activity has risen, which arises due to individual neglect or carelessness, such as opening a phishing email or losing storage devices [21]. These are just as important to organizations as they are occurring more significantly than intended malicious activity [22]. They generally do not have any malicious intent to harm the organization. However, any harm causing may lead to sensitive information leakage and/or unauthorized access to outsiders.

There is another factor, "workplace violence", that can influence the working behavior of the employees. This is evident in the practice of physical attacks, threatening or inappropriate behavior and speech (written or verbal), harassment, resource damage, or other actions that could place fellow employees at risk. According to a Federal Bureau of Investigation report [23] on behaviors of active shooters, 62% of the people who went on to become shooters were previously involved in a harassing, abusive, or oppressive manner. Early signs for workplace violence include insults, passive-aggressive activities, dramatic or irrational demands, and unexpected and unjustified whining or complaining [24]. Possibly, the insider intends to gain some benefit by harming other employees. However, workplace violence is not in scope and will not be addressed in the paper in detail.

3. Attack Vectors and Techniques

It is paramount for enterprises to identify the technologies, tools, and practices that cybercriminals use to implement insider threat attacks. This is due to the potential destruction they cause—examples include suspension of operations, loss of intellectual property, and reputational harm as they have easy access to systems and a greater window of opportunity to infiltrate. Through

insider threat incidents, the practices of insiders can be identified and consequently combated with suitable defenses. This section will identify common methods cybercriminals use of insider threats to compromise an organization's network environment to gain access to valuable assets.

3.1. Privilege Escalation Techniques

The compromise and subsequent misuse of privileged access accounts have shown to be a typical trend within major insider security breaches [25]. A privilege escalation attack is a technique that grants an attacker elevated access to protected sensitive resources by taking advantage of design flaws or configuration errors. This can be achieved via two methods: vertical or horizontal privilege escalation. Vertical privilege escalation involves the attacker granting himself higher privileges usually created for higher-access users [26]. This allows the insider to execute unauthorized actions to manipulate the information system. An attacker can typically accomplish this by executing kernel-level operations allowing unauthorized code execution [27]. Horizontal privilege escalation involves the attacker using the level of accesses they have been granted but assumes the identity of someone with similar privileges to gain access that he may not have [28]. For instance, Internet of Things (IoT) devices, such as intelligent electronic devices (IEDs) can be accessed by a group of people with a specific role (e.g., vendor engineer or management personnel) in the industrial control system (ICS). Therefore, if an insider can compromise and escalate his credentials, he can disrupt and modify critical systems to gain access to assets. There are several privilege escalation methods, using which the insiders can get access to the required resources. This also includes access token manipulation (e.g., copying an access token, developing a new process with an impersonated token, leveraging username and password to generate a token), bypass user account control (e.g., execute component object model (COM) objects with administrative privileges without permissions), and dynamic-link library (DLL) preloading (e.g., placing a malicious DLL in the system to execute).

3.2. Exfiltration Attacks

The objective of insider threat is to locate the "crown jewels" and move the jewels out of the protected network. This is referred to as data exfiltration which is defined as "the unauthorized copying, transfer, or retrieval of data from a computer or server" [29]. The methods for transferring this data outside of the protected areas include overt, tunneled, or covert channels [30]. Overt channels are accredited open communications that involve a level of trust within an organization. Examples include Cloud sync storage, such as the internet file hosting service Dropbox or FTP that is used to send files off-site. Hence, a malicious insider can use Dropbox to copy files and then immediately delete them from the folder. As a Dropbox user, even when you sync and delete a file from Dropbox, that Dropbox keeps a copy of that deleted file for 30 days for retrieval. Thereafter, he can recover the files from an external location. Furthermore, insiders can gain access to the targeted system of a more physical nature via removable USB devices [31]. They can be used to exfiltrate sensitive information from network endpoints whilst being concealed due to their size. Additionally, they can introduce malicious code onto a network endpoint that compromises the confidentiality, integrity, and availability of sensitive information [31].

3.3. Phishing Emails and APTs

UIT can cause substantial harm to an organization's information system. An outsider cyber-criminal can take advantage of an insider through techniques such as social engineering (phishing emails), an attack vector in the art of manipulation, and network attacks such as APTs [32]. Attackers can gather company email addresses to send spear-phishing to attempt to infect specific or generic insiders. For example, most organizations have generic email addresses for their employees. Once the attacker has figured out the algorithm for the company addresses, they can reach a plethora of users [33]. Furthermore, social networks such as LinkedIn will also offer a range of users for an attacker to choose, as they provide easily accessible email addresses [34]. Moreover, social media sites like Facebook and Twitter make it effortless to gather personal information that can be used in

custom-tailored emails that will elicit the trust of a victim [35]. For instance, the software company Sophos found that 40% of social media users have been infiltrated by phishing attacks [36]. Hence, these practices cybercriminals use have demonstrated considerable ingenuity and refinery in formulating these emails to insider personnel.

As aforementioned, APTs are sophisticated technologies that cybercriminals use to break into systems, stay hidden within networks, and keep long term access to data. APTs leverage insider threat as cyber-criminals focus on using the hijacked credentials of current employees or business partners to compromise targeted systems of valuable data [37]. Furthermore, an unintentional insider (UI) can fall victim to an APT by being utilized as an information harvesting point. A UI may have been convinced to click on a malicious link that delivers the APT, acting as an entry point, and granting full access to network information [33]. A key factor in the success of these attacks is that traditional network systems cannot detect these types of threats. For instance, threats exploiting zero-day vulnerabilities cannot be stopped by the widely expanded signature-based endpoint security products as the signature is not readily accessible yet. Likewise, the security firm Mandiant indicated that 100% of insider attacks had anti-virus perimeter security in place [38]. Thus, emphasizing the need for security and awareness training for UIs to be aware of this risk as opposed to technical security.

4. Cyber Kill Chain

For a malicious insider to proceed and execute an attack, there are multiple steps that need to be completed [4]. These steps adapted by Lockheed Martin are the 'kill chain' [39]. Stopping attack at any stage results in the disruption of the whole attack. Hence, improving defense threat intelligence at all phases of the kill chain allows a defender to deny future attacks earlier on in the kill chain. It should be noted that the cyber kill chain was initially proposed for analyzing external threats. It was, however, noted in this work that the kill chain can be an efficient approach for studying the internal threat.

4.1. Reconnaissance

The initial aim of a malicious insider to undertake is a search for valuable data. This reconnaissance phase involves investigating within the systems they already have access to or to find systems that can gain access to the valuable data [40]. It could begin as a curiosity about where their access boundaries lie or accessing information that is not relevant to their position. The insider could ask co-workers vague questions about the organization, conduct searches on data, or delegate data to another individual. The malicious insider can achieve this through privilege escalation techniques such as vertical privilege escalation [26]. For example, a malicious insider who has gained unauthorized access to a user account can see what the compromised user can do and what systems they have access to. The user may be able to download the software freely or write scripts from this account. This gives rise to potential exploitation as they could find a vulnerability or configuration errors to become an administrator of the computer system. Moreover, companies can ignorantly reveal knowledge about their businesses that can be exploited for a cybercriminal's advantage [33]. For example, corporate websites can disclose information such as contact addresses and partners' information which can be profitable for an attack. Additionally, press releases and public white papers also provide advantageous information on what anti-virus software the company is using, alongside the names of the academics involved in their research. From this, a malicious insider can learn the target's activities as they show what work is done within the company. They also show the template for the company's publications; these could be used to design fake documents that could trick employees [33]. Furthermore, employees often leak sensitive information without knowing it via social networking sites, typically stating their employer's name giving rise to target identification. An insider can find sensitive project names and gain more information on specialists who want potential recruiters to see their profile on LinkedIn.

Moreover, dating applications may be used by employees within organizations. An external attacker could cross-reference LinkedIn or Facebook to "catfish" or manipulate an employee involved

in critical infrastructure into acting as an insider threat [41]. Although, organizations cannot regulate the personal lives of employees, yet the critical infrastructure entities should consider when reviewing applications possible insider polarization vectors. To mitigate the reconnaissance phase for insider threats, organizations need to prevent insider radicalization due to perceived personal bias or chilling effects. The personnel needs to be repeatedly informed of their privacy rights in the workplace through training, login screens, and signs and that their activities are constantly being monitored. Moreover, users should know a clear chain-of-command and should have access to a reporting mechanism to testify any suspicious insider activity.

4.2. Weaponization

This phase involves the insider creating a "remote" access malware weapon (e.g., Citadel for stealing the credentials) tailored to a specific vulnerability within the company. The Citadel malware has been used to steal online banking credentials and other financial information by altering the website on the fly in a local browser at the user's end. In many cases, insiders directly exploit vulnerabilities already existing in the targeted systems (e.g., web application vulnerabilities). In some cases, insiders can use tools already available in the organization for their attacks. We use the term "remote" to refer to the type of exploit rather than the location of the attacker, which in this case can be within the organizational infrastructure, as well as an external who may be colluding with an employee. Typically, application data files such as Microsoft Office or Adobe Portable Document Format (PDF) serve as the weaponized deliverable [39]. An attacker, if successful, can implement an APT with an infected PDF file to a targeted insider. Moreover, the APT relies on targeting unintentional insiders with watering hole attacks, spear-phishing, and drive-by infections to push their malware onto the targeted infrastructure. If malware on an organization's system records the password, then this can provide attackers with the key to information systems. To disrupt this phase of the kill chain, two-factor authentication could be implemented that involves password systems that require a second step, such as answering extra security questions.

The malware can be transferred onto a USB drive despite cybersecurity awareness and training, is to plug a lost USB drive into an organization's computer system to identify the owner [41]. These forms of social engineering attacks can be implemented by nation-state ATPs to infect the corporate's critical infrastructure through an un-cyber-hygienic employee. This form of infiltration occurred in 2008 where the Agent.BTZ malware was spread through the Department of Defense critical infrastructures. Agent.BTZ (aka, Autorun) is a worm that principally spreads itself via removable devices such as USB drives with spyware. This worm propagates by making an AUTORUN.INF file to the root of each drive with the malicious.dll file. The malware was reportedly spread by the Russian state-sponsored Uroburos APT. The Uroburos malware scans for the presence of Agent.BTZ on target systems and remains inactive if Agent.BTZ is present. The Uroburos malware is sophisticated as it is designed to infiltrate an entire network and extract the data back to the attacker. The malware can also infect air-gapped systems such as infecting transient host systems and USBs. One of the most dangerous weaponization examples of insider threat is a malicious nation-state sponsored APT proxy that compromises sensitive data from an organization as part of a multi-vector warfare campaign. For example, Securonix Chief Scientist Igor Baikalov, an ICCIT Fellow quotes, "We do see quite a bit of employees offering their corporate credentials for sale advertised on the dark web—is a lot cheaper and faster than hacking your way into a corporate network and then looking for the right level of access. Besides willing insiders, coercion in the form of blackmail, extortion, and other threats has been made easy by the availability of massive amounts of very sensitive information from the breaches at the U.S. Office of Personnel Management (OPM), Anthem, Yahoo, and others." From this, nation-states could build pertinent profiles for potential targets.

4.3. Delivery

This stage involves the transmission of the weapon to the intended target through different steps. This may involve only a few steps if the attack is straightforward. For example, when an insider just gets hold of some assets to whom he has access or by compromising the credentials of some

colleagues to get access. However, in many cases, the insider carries out a sophisticated attack that requires many steps, which may require an insider to exploit several vulnerabilities, perhaps inject some code and so forth.

The attack vector in the former case would involve an exfiltration attack. For example, the insider would use a USB device to upload potentially damaging malware to the organization's systems either unintentionally or intentionally [42]. Moreover, an insider could use Dropbox to copy files and access them from an external location. Furthermore, the attacker could send infected emails in a phishing attack [22]. They could customize email messages using social engineering techniques via social media accounts to target insider employees and business associates. To disrupt this step in the kill chain, the staff needs to be trained to recognize and report these phishing emails. In the latter case, the attack vector would involve several complex steps [43]. For example, an insider can install malware that could steal the credentials (e.g., Citadel, through an email phishing campaign). Once an insider does that, he can use this stolen information to gain access to target a hosted web service dedicated to vendors.

Now, to execute a command on an application, the insider is required to compromise the machine. To do that, the insider exploits a known vulnerability (e.g., web application vulnerability such as "xmlrpc.php" is used to execute scripts within web applications) and look for the relevant target for propagation (e.g., doing reconnaissance to locate and identify the server holding customer information, e.g., credit card, human resource documents, and other confidential information). On Windows, this can be done through querying Active Directory with internal Windows tools using the standard Lightweight Directory Access Protocol (LDAP) protocol. Move on, once the insider has identified the target, he looks for access privileges (e.g., domain admin privileges using a well-known attack technique called pass-the-hash to gain access to an NT hash token) to affect it. Lastly, the insider creates a new account using the stolen privileges and adds this account to the domain admin group.

4.4. Exploitation and Installation

The exploitation stage is where the malware's weapon program code activates, targets, and exploits the network's vulnerability. For example, an insider can still exploit the vulnerability by privilege escalation methods such as accessing someone else's user account that has lower privileges than themselves [28]. Installation of the remote access allows the adversary to maintain persistence inside the environment. Hence, a developer could modify the source code or introduce malware that will inevitably harm the organization. For example, they could infiltrate a code into a system and the execution of the code could cause databases to be destroyed [44]. Additionally, an insider could interfere with data by creating unauthorized changes of the deletions, making the data inoperable. This method involves slowly destroying data over time, by the time the company notices, these restoring backups are also damaged, which sets the company back drastically.

For example, system administrators, who are privileged users, have authority and access to sensitive salient data and can turn rogue with severe consequences. Such as, a network administrator locked the city of San Francisco out of the FiberWAN network. This network served as the infrastructure that governed police records, payroll, and city hall systems. The administrator had become disgruntled as he felt that his job was in danger that he locked the system. A rogue system administrator could deploy malware or Ransomware onto critical infrastructure. For example, in 2015, the BlackEnergy malware attacked several Ukrainian power plants. The system administrators were targeted by a phishing email that loaded the malware onto the system for which the attackers could gather credentials and gain control of the electricity systems.

4.5. Command and Control (C2)

The Command and Control (C2) phase is where the insider takes over the system in the targeted environment. In traditional systems, C2 infrastructure may be absent or is not required to perform a simple insider attack. However, to perform complex and APT related insider attacks, this is required. An employee who has access to the system control and data acquisition (SCADA) interfaces can

control the industrial systems giving rise to potential destruction by mishandling his access to these systems [44]. As such, if an insider worked in a dangerous chemical plant, he could control the valves that aid the release of poisonous chemicals into the environment. Furthermore, employee negligence can lead to remotely accessing computer systems. They could do this by connecting to a public Wi-Fi area where there is an insecure network but that could be compromised by an APT designed to target negligent employees. For example, in 2013, an American software developer outsourced his job to a consulting firm in China. The negligent insider surfed his social media and emails during his working days for which his credentials were being used to remotely access the company systems. This means that a foreign agent could access that organization's data and systems for malicious intent.

4.6. Intrusion and Takeover Complete

At this stage, the insider works to achieve the objective of the attack, including data acquisition and exfiltration, the elevation of privileges, or the possible intrusion of another target. For instance, an insider may use privilege escalation once more to consider other possible systems that contain valuable data. Through this demonstration of insider threat attacks and their relevance to the kill chain, is the presentation that insider threat can extend and blend throughout all phases of the kill chain. As both technical and non-technical tools can be executed for an insider to compromise an organization, the kill chain is especially relevant for vigilant preliminary defense strategies to be distinguished at the stages. Now, Table 1 shows scenarios for insider threat activities in line with different phases of the cyber kill chain method where the operator's activities denote insider threat behavior.

Table 1. Insider threat and kill chain method.

Stage	Insider Activities	Tools/Techniques
Recruitment/ Tipping	An engineer hands in his resignation, unknown to his team at the time he was leaving to resume duty with a competitor.	Email or paper.
Reconnaissance	For four months, the engineer visited some network shares on the system that contain data from different divisions of the organization. He explored several areas for accessing documents, opening files, and browsing directories.	PCs, browsers, webpages, ping sweeps, social networks, port scanning, network sharing, Telnet/R-login.
Exploitation	The organization did not control the critical and sensitive zones of its network with the correct level of permissions. Therefore, open and free access to data and information was available to those who have access.	Remote access tool (RAT) and exploit kits, particularly, Blackshades—Blackhole; DarkComet—Nuclear; Bozok—Redkit; Poison ivy—Styx; Njrat—Sweet orange; Apocalypse—Infinity; and Browser exploitation framework (BEF).
Acquisition	Once the engineer had discovered the data he wanted to steal, he downloaded a piece of software that is designed to create backups. He installed it on his system and configured it to retrieve the needed files from the network and secure them in a single file. He was sensible enough to configure the software to perform incremental backup after the initial backup. This means if there is any change or addition to the file location, the software will only add the new changes.	Backup software—Acronis True Image, EaseUS ToDo Backup, Paragon Backup & Recovery, NovaBackup, and Genie Timeline.
Exfiltration	Once the engineer was done, he unplugs his endpoint from the network and copies the backed-up file to a drive.	USB thumb drive, Hard disk.

5. Defense Strategies

The insider threat is a complex problem, with many researchers proposing a layered defense approach involving policies, procedures, and technical controls. Based on the ENISA report [4], the following elements contain the best practices for defending and combating the risk of insider threat. Table 2 summarizes the potential targets and associated defense approaches.

Table 2. Summary of defense strategies.

Strategies	Authors	Targets	Defense Approaches
Definitions of security policies regarding insider threats	Omar [1], CERT Common Sense Guide to Mitigating Insider Threats [45]	Gaps in policies	Concise and coherent; penalties for violating rules
Pre-employment and monitoring suspicious or disruptive behavior	Shaw et al. [46], Greitzer et al. [47]	Non-trustworthy candidates, disruptive behavior	Background checks, enforce policies and procedures
Prevention of data exfiltration methods	Hunker et al. [48], Scott et al. [41]	Data leaving critical systems (copied, transferring, USBs, etc.)	Shadow copy creation, audit media devices, virtual desktop infrastructure environments, data loss prevention
Strict access controls and monitoring policies for privileged users	Giani et al. [30] Oracle Database Vault [49]	System administrators and privileged users, sabotage previous employees	Disable system access for required users, strict encryption solutions, principle of least privilege, protect user data from DBAs
Separation of duties	Cappelli et al. [14], Iyer et al. [50]	Privileged users, system misconfiguration	Strict organizational rules, collaborative network systems
Segregation of duties	Moore et al. [51]	Authentication attempts suspicious activities	Audit logs, dashboards, alerts, and alarms for security analysts to inspect
Indicators of compromise	Mihai et al. [52]	Intrusion kill chain	Use of a security incident and event management (SIEM)
Human behavioral and psychological approaches	Greitzer et al. [53]	Unintentional insider threat (UIT) from social engineering	Collecting and analyzing the data for behavioral and patterns
	Liu et al. [11]	Range of insider threats (mostly the traitor, masquerader, and unintentional perpetrator)	APT intrusion kill chain
	Nurse et al. [22]	Motivation behind malicious threats and unintentional human factors	Technical and behavioral aspects
	Chen et al. [54]	Insider threats based on the access structure	Community anomaly detection through logs of collaborative environments

5.1. Definitions of Security Policies Regarding Insider Threats

A non-technical defense measure is enforcing consistent and clear security policies to employees of all levels of the organization [1]. Insiders will exploit any gaps in policies to damage the organization, therefore ensuring the policies are concise and coherent with emphasis on the reason behind the policies is essential. Moreover, if these policies are misunderstood or not received consistently, then it can result in insider disgruntlement and promote malicious activity. A common practice that organizations use is that all employees receive and sign a copy of these policies. Through this, the employees are made aware of what is expected from their job roles and the penalties for violation of these policies are clearly agreed upon [45].

5.2. Pre-Employment and Monitoring Suspicious or Disruptive Behavior

The first line of defense to mitigate insider threat begins at the hiring stage. Potentially non-trustworthy candidates can be identified at the application stage by conducting background checks such as criminal convictions, credit issues, verification of credentials, and previous employment regarding competency [4]. Provisions need to be enforced not just for employees but also for contractors and subcontractors who need to be investigated under the same scrutiny. A common practice for organizations is to train managerial roles to recognize inappropriate behavior of employees. They can consistently enforce policies and procedures and respond to any act of violation [46]. Moreover, if financial gain is a primary motive for an insider, then abrupt changes in an employee's wealth could be a sign of potentially malicious activity [47]. Furthermore, policies regarding the reporting of disruptive behavior of a co-worker can help in defending against the insider threat.

Sometimes, those mitigation strategies can carry significant costs to an organization which is why strategic investment needs to be implemented in securing highly sensitive resources. Research has indicated that there is apprehension over the inefficiency of cyber security investments [55]. The investments are measured in isolation of other current investments within the organization. However, increasing the amount of investments tends to have a diminishing benefit beyond a certain point. It is argued that the current investment models rely on an expected value as opposed to a probability distribution of an outcome. Moreover, these investments assume that the mitigations are independent with drastic preventative effect.

5.3. Prevention of Data Exfiltration Methods

To prevent data exfiltration attacks, organizations need a thorough understanding of where and how data can leave their critical systems. Different device types (e.g., Android devices for covert data exfiltration) that are used for exfiltration can present different challenges, but there are methods to control and audit these media devices. For example, Microsoft Windows has developed group policies where administrators can determine which devices can be installed on systems [56]. Furthermore, some organizations have developed features onto their systems where, if files are moved, a shadow copy of that file is automatically created [48]. This can determine who has copied the file and what contents the file has within it. To help mitigate this risk further, companies should allow for company-owned removable devices that are encrypted before a file is moved to it [45].

To disrupt the delivery step in the kill chain, virtual desktop infrastructure (VDI) environments can circumvent the delivery process. This is where all data are stored onto remote servers and that the user only interacts with a local application on the computer. Through this, an insider cannot download any data or perform an exfiltration attack. A system administrator can concentrate on managing and securing the servers with the users being held responsible for their desktops. Moreover, the features involved in digital rights management (DRM) can be implemented to detect any form of data leak through watermarks or print prohibition controls [41]. Furthermore, data loss prevention (DLP) is where vendor tools are securing the data when it is in transit, rest, and at endpoints. It may also include network monitoring and involve mechanisms to deter any threats. However, DLP is not sufficient enough for the evolving threat of insiders as it was not built with

insiders in mind. A determined insider threat actor will be able to circumvent the controls involved in DLP. Therefore, by implementing user activity monitoring (UAM), organizations can identify any suspicious behavior and mitigate any risks whilst maintaining business continuity. Through this user-centric method, any suspicious behavior can be extracted by case-by-case analysis.

5.4. Strict Access Controls and Monitoring Policies for Privileged Users

For an organization to mitigate the risk of insider threats, they must guarantee that their system administrators and privileged users are to be trustworthy. Many individuals who commit insider threat sabotage were previous employees; therefore, organizations must disable system access for these users once they have left the company. Besides, organizations should implement strict encryption solutions before allowing privileged users access. This is due to privileged users having access to encryption tools which pose a risk as they could encrypt valuable information (claiming as their personal information) and decline to produce the key [45].

Furthermore, a key factor that influences the success of privilege escalation with insider threat is the principle of least privilege (POLP) [30]. This involves the operation of every program and user using the least amount of privilege necessary to complete a task. Through this, the attacker may not be able to reach beyond that user's privileges despite having full access to an individual user account. They must escalate through other ways, such as a faulty program that operates at a higher level of privilege. Therefore, POLP produces several layers of complexity and reduces the likelihood of the attacker's success. In this direction, Oracle has a product called Oracle Database Vault, which is designed to protect user data from Database Administrators (DBAs) who are typically high-privileged users [49].

5.5. Separation of Duties

Another process that organizations use to mitigate against this threat is the implementation of separation of duties for all roles including privileged users with at least two people needed to alter modifications on the system. From the list of controls produced, strict access controls and monitoring policies for privileged users is of great importance. This is because of the increased risk they pose to an organization's valuable data due to their technical ability and the easy concealment of their actions in modifying systems. To prevent this, organizations have used non-repudiation methods (signatures or certificates) to monitor single employee's online activity, regardless of their level of access [14]. Therefore, organizations can access information to demonstrate who has been conducting malicious activity. They can achieve this by configuring systems to enable non-repudiation methods via policies and technologies. Yet, these methods tend to be designed by current privileged users such as administrators. To overcome this, organizations have established that multiple privileged users should develop network systems collaboratively. Moreover, organizations can observe that their employees are only accessing the necessary resources involved in their job role. They achieve this by thoroughly checking employees' daily activities (based on their role and tasks assigned) and any activity outside their boundaries can be deemed as suspicious. Also, this relates to the principle of least privilege where strict organizational rules let employees have access only to resources that are required for their job role [50].

5.6. Segregation of Duties

The segregation of duties refers to the assignment of steps in a process that eliminates instances where a person can have an excessive amount of control over the process. This may lead to theft or other fraudulent attacks. To further control access management, organizations can implement segregation of duties [4], for example, per defined roles. They can achieve this through protocols and technical means, for which some systems require multiple users to modify information systems. For example, someone could raise a purchase order for £2 million, but they would not be able to approve it. Thus, a senior manager with approver roles will only have the authority to approve it in their cost center and the application database will audit this event. A single worker should not be able to make

any changes to any technical system without the permission of another. As such, a peer review of a developer's code can be applied to reduce any risk of malicious activity. Hence, organizations should have at least two system administrators to reduce and combat this risk. Furthermore, organizations rely heavily on audit logs to identify authentication attempts that are collected and analyzed to show any form of suspicious activity [51]. The auditing role can be separated from a single administrator to enforce separation of duties and to reduce the risk of an organization becoming victimized by a sole administrator. From a technical point of view, Table 3 provides examples of security information and event management (SIEM) actions. Following the process of a kill chain, organizations need to put controls and stoppers in place that could flag any unusual occurrence as a way of dashboards, alerts, and alarms for security analysts to inspect. Furthermore, the system and network should be fortified to stop and disallow the process of kill chain by an attacker. Access control lists (ACLs) are used to filter the network traffic that controls incoming or outgoing traffic from source to destination through setting a set of rules on whether to forward or block a packet at the router's interface. This brings a matrix (shown in Table 3) for action by the United States Department of Defense.

Table 3. Matrix for action.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Website Traffic	Firewall Access Control List (ACL)	-	-	-	-
Weaponization	Network IDS	Network IPS	-	-	-	-
Delivery	Cautious User	Proxy Filter	In-line Antivirus	Scheduling in Queuing	-	-
Exploitation	Host-based IDS	Patch	Data Execution Prevention	-	-	-
Installation	Host-based IDS	Modified system	Antivirus	-	-	-
Command and Control	Network IDS	ACL	Network IPS	Tarpit	DNS Redirect	-
Action on Objective	Log files	-	Network IPS	Quality of Service	Honey Pot	-

5.7. Indicators of Compromise (IOC)

A major goal of the kill chain is to map the intelligence and tools available in an organization environment with the actions conducted by the insider [52]. However, the implementation of the matrix of action may indicate a secure environment, but more pertinent is the recognition of a zero-day exploit. With the use of a security incident and event management (SIEM), intelligence can be gathered about specific indicators of compromise (IOC) that will allow the security analyst to track the insider staff activities. These indicators of compromise can be human or technical, a few examples of which are given in Table 4. The first step in using a SIEM tool is to set a baseline to determine what is normal and abnormal. Besides, it is necessary to determine what information needs to log on to the SIEM tool. A few examples are:

1. Record of physical access to the office areas including restricted and sensitive areas,
2. Record of access to hosts and servers,
3. Database activities,
4. Vulnerability data,
5. Individual user activities,
6. Configuration data,
7. Security device logs,
8. Application activity logs,
9. Active directory.

Table 4. Indicators of compromise.

Indicators of Compromise (Insider Threat)	
Human	**Technological**
12 months plus unused vacation	An increasing # of logins, variation in remote/local
Consistent first in and last out of office	Logging into the network at odd times
Life change/marital status	Remote logins using employee credential
Lay-off notification	Changes in website visited work and personal
Passed over for promotion/raise	Increased printer usage
Disciplinary action	Export of large reports/downloads report

A SIEM signature can be generated for insider attacker logging to account outside office hours through common event format (CEF) or common event expression (CEE). The signature may include the details depending on the event standard in use, such as username, virtual private network (VPN) account name, hostname, and remote connection protocol.

Another important IOC to detect potential malicious insiders is anomaly detection (AD). This is especially helpful in scenarios where it is difficult to detect an insider using traditional and straightforward approaches. Using AD, one can detect anomalies in the user's patterns. For example, an employee for his daily tasks' accesses 20% of a table; then one day this employee downloads the entire table and copies it into a file. This is a clear anomaly that may indicate an insider attack. Of course, being an anomaly there could be legitimate reasons for it. However, flagging it is important.

A risk rating is then assigned to the risks involved and risk scores can be increased by the magnitude of deviation from normal activities and the sensitivity of assets involved. A list of suspicious or monitored users can also be created and placed on a dashboard. Any spike on the data generated on the dashboard by a suspected user profile can indicate a possible intelligence on a possible threat, which should be investigated and monitored. An organization can also create alerts and alarms on possible threats or compromise of the systems or network and create automatic responses. A SIEM signature can be created to achieve this task. SIEM signatures should be assigned to individuals that require monitoring to reduce false positives [57].

5.8. Human Behavioral and Psychological Approaches

To better comprehend the respective threat of insider activity, three elements need to be considered. One such element consists of the psychological factors involved in these attacks, and what impact technologies, such as social media, have on insider attacks.

Greitzer et al. [53] addressed the unintentional insider threat (UIT) cases that can be derived from social engineering exploits by collecting and analyzing the data from UIT social engineering incidents to recognize the likely behavioral and patterns. Recent attacks, such as the U.K. National Health Service WannaCry ransomware attack which partly depends on internal users for initial infection, highlight the increasing role of the malicious insiders in cyber-attack campaigns [58]. The literature evidence suggests that there is high heterogeneity across crude data, indicating that the effectiveness of security measures varies significantly, and no solution can mitigate an insider threat. Liu et al. [11] extended the range of insider threats (mostly the traitor, masquerader, and unintentional perpetrator) by involving those relevant early-stage threats which are all lined up with the APT intrusion kill chain. Nurse et al. [22] proposed a framework that identifies the key elements which concentrate not only on the noteworthy events and indicators, i.e., technical and behavioral aspects of the potential attacks, but also on the motivation behind malicious threats and the human factors related to unintentional ones. Chen et al. [54] introduced a community anomaly detection system (CADS) that detects insider threats based on the access logs of collaborative environments and based on the observation that typical users follow community structures based on the subjects accessed.

Psychosocial behaviors to be analyzed include lateness, absenteeism, unruly clashes with co-workers or superiors, disregard, disgruntlement, performance stress, and self-centeredness. Such employees can perpetrate sabotage by spoofing, misuse of computer functions in creating a back

door, executing unauthorized software scripts on the organization systems. This information can be recovered majorly from co-workers and human resources.

Exploring the human and psychological factors involved in insider threat needs to be critically considered. For instance, Shaw and Stock [46] found that insiders who score higher on personality traits such as narcissism are more likely to cause malicious activity. Moreover, research has established that certain behavioral traits need to be measured; these include arrogance, self-centeredness, and risk-taking [59]. If specific traits are related to insider threat, then prevention and deterrence of any activity taking place can be implemented. Furthermore, research has shown that emotional states and psychological disorders of employees can aid in malicious activity [60]. For example, in cases of extreme stress, a financial crisis can exuberate malicious behaviors [46]. Additionally, people with psychological disorders such as addiction (gambling) are more likely to engage in malevolent activity than those without a psychological disorder [6]. This highlights the importance of understanding complex human behaviors within corporate environments and how it can support the identification of suspicious data handling by an insider.

The criticality of insider threat also involves the use of technologies such as personal devices and social media. Even though the use of personal devices has grown in popularity, they come with an increased risk of fraud [17]. Despite whether personal devices reduce the cost of supplying company-owned devices, organizations need to deliberate whether it is worth the risk of severe data breaches. Moreover, social media is critical in the development of insider threat risk as attackers can locate sensitive information that can be used to their advantage. This creates a high vulnerability risk as organizational campaigns can be accessed with vital information on trade secrets. Besides, external outsiders can use target identification to exploit possible insiders. Thus, organizations should not underestimate the effect of social media [35].

Mostly, detection techniques are based on the technical aspects. Therefore, it is required to fill a gap in detecting insider threats by the current tools, such as user activity monitoring (UAM) and user behavioral analytics (UBA) [61]. Cassidy [61] developed a factor-tree model of the incident (intended harm) lifecycle that can be used to systematically generate scenarios across five states: predispositions, stressors, grievances, ideation, and planning and prep.

5.9. Organizational Risks and Ethical/Privacy Considerations

Organizations must understand the criticality of insider threat, as the associated risks can be detrimental. However, organizations are more concerned with outside rather than inside threats as the enemy is perceived as beyond the organization. This is evidenced by the lack of investment used in insider security. For example, the State of Security report [62] found that corporations only spend around 11% of their revenue on security defenses aimed specifically at mitigating insider threat. Considering the amount of risk involved, this is an insufficient amount of investment needed for the prevention and detection of these threats. Likewise, companies are not going to invest more money into defending against this threat if they believe it to be insignificant. For example, Ponemon's survey found that although 61% of employees feel that insider threat is a high risk, only 44% believed their company puts insider threat as a top priority [63]. This emphasizes the fact that organizations perceive themselves as ill-equipped yet are unmotivated to activate risk management. Moreover, corporations deem that the probability of being attacked as low risk, which has detrimental effects on any protocols being implemented in protecting against the insider threat.

Another organizational aspect of insider threat can be shown through how companies deal with the threat once detected [22]. Kaspersky [10] found that these incidents are under-reported and that no notification was given outside the boundaries of the organization. It was identified that organizations are not responding appropriately as they do not have a clear understanding of the associated risks. Most likely proposing that organizations can develop their understanding by researching current and past threat landscapes such as the ENISA Threat Landscape [4]; these landscapes summarize the most prevalent cyber threats with strategic mitigation vectors for the respective threat.

Another important aspect is ethical and privacy considerations for insider threat detection. In this direction, Rashid et al. [64] suggested educating individuals to report certain behaviors that they perceive in their peers. These "characteristics of insiders at risk of becoming a threat" are imprecise (ethical flexibility, introversion, etc.) and can often be tough to quantify. At times, information security challenges shoot from inconsistent and differing technological standards. However, it has more happened because of the lack of awareness in understanding several ethical and social norms from one location to another [65]. Further, Greitzer et al. [66] explored social and ethical issues stemming from predictive insider threat monitoring and resolved by stakeholders and communities of interest.

When an insider is violating ethical standard practices in the organization, he risks users' private data, identity, and assets associated with that identity. Following unethical practices (intentionally or unintentionally) may also lead to severe consequences, such as leaking data to competitors, disrupting internal processes, or potentially bringing the whole business to a halt. It could be a great challenge to monitor and detect insiders without violating privacy laws and policies.

While these policies are straightforward, there is a strict requirement of following the data protection requirements, such as due to the General Data Protection Regulation (GDPR). In general, for monitoring purposes, it is important to explicitly notify the employees that they and associated devices and resources are under the surveillance system to maintain data protection. In order to monitor and maintain ethical and privacy considerations, a rigorous information security policy is required to implement. Additionally, various internal processes are required to prevent unethical actions from insiders. For example, when developing software, it is helpful to have an inclusive history regarding the developers' involvement and actions to the application, standardized code review practice, code change approval progression, and continuous static code analysis helps in detecting the unethical behavior among developers [67].

5.10. Detecting Insider Threats by Monitoring Disruptive Behavior

As previously mentioned, there are many different methods for detecting insider threats.

5.10.1. Detection by Monitoring Disruptive Behavior

From these techniques, there is a clear indication that many of these attacks are detected through nontechnical means such as the monitoring of disruptive behavior of co-workers. Furthermore, Kaspersky [10] found that 47% of insider threat cases were reported by co-workers identifying disruptive behavior, so the education focus and awareness within organizations need to be encouraging employees to engage in this security domain [22]. Therefore, companies need to develop and build suitable defenses, incorporating the identification of co-worker behavior. Likewise, PricewaterhouseCoopers (PwC)'s cybercrime survey [63] has identified that some organizations have included three elements for detecting and identifying insider threats. These include corporate controls (identifying and monitoring suspicious transaction behavior), corporate culture (reporting misconduct), and those not under the influence of management (third party or accidental discovery). At every period end, a business information report is created, which will highlight untrustworthy financial purchases that can be reviewed. They found that from 2005–2011, suspicious-transaction monitoring increased by 18%, and with that, methods such as whistle-blowing led to suspicious behavior being relayed to management. This emphasizes how critical these detection methods are for insider threats. However, Kaspersky's [10] survey identified that information technology personnel reported 41% of irregularities in activity logs, signifying that non-technical defenses alone do not identify threats.

5.10.2. Detection by Automated Tools

It is also important for organizations to identify current automated detection software tools that can apply many prevention methods in one [63]. For example, Forcepoint insider threat by Raytheon is a new commercial software tool that can detect, prevent, establish, and identify suspicious activity

to reduce and stop data loss. For instance, the Command Center provides highly intuitive systems to identify any uncertain behavior that will heighten the risk of insider threat, whilst controlling what data to specifically collect from users. Thus, it is essential that corporations invest in technical defenses as well as non-technical to increase their breadth of security and reduce their overall risk. It is evident that monitoring the activity of employees and applying the segregation of duties is essential for insider risk management. This can be achieved by anomaly-based approaches, which can establish what normal activities the user is involved in [68]. However, these approaches can result in multiple challenges. For example, measuring the amount of deviancy needed to be a malicious insider, or to determine what the normal behavior against abnormal behavior is, if there is already a malevolent insider within the organization presents difficulties. Moreover, employees' daily routines could change and vary depending on the demands placed on them including workload. Therefore, they could be asked to work longer hours or complete tasks dedicated to other employees, particularly if other employees are on leave, then workload will need to be covered. Hence, the anomalous behavior will be flagged as malicious and yet the behavior is not. Organizations should develop a system by careful management as employees can be accused of being a threat, representing the challenges involved in building strong suitable defenses for insider threats.

Other challenges are involved in automated threat detection systems, including false alarms. This can result in a loss of availability where employees cannot gain access to the system and effectively complete tasks during a time-sensitive emergency. A loss of system availability can become a costly burden to an organization. Furthermore, the reputational damage of the organization can be compromised, including loss of revenue. Loss of availability, confidentiality, and integrity establishes a security breach. Strategies to reduce these errors involve using other models, including the intention model. This model is used to assess probable threats based on the psychological profiles of insiders. When an anomaly is detected involving the insider's behavior, the intention model looks at the motives behind a user to see if they have any malicious intent. If there involves a substantial amount of motivation and interest, only then can the alarm be raised.

5.10.3. Detection by Human Signals

There is the current state of the art research into developing suitable defense systems due to the severity of insider threat. One example of this comes from researchers Hashem, Takabi, Ghasemigol, and Dantu [69] as they applied the use of human bio-signals in detecting malicious insider activity. They developed a framework for insider detection with 90% accuracy using electroencephalography (EEG) and electrocardiogram signals. This suggests that the brain and heart signals reveal information about malicious behaviors and could be an efficient solution in detecting insider threats. However, as acknowledged by the authors, it is inconvenient and unrealistic for users to wear the device all the time. Yet, this may not be an issue for the future as technology has already adapted smartwatches that can measure EEG signals.

Axelrad et al. [70] introduced a Bayesian network model for the motivation and psychology of the malicious insider. Their work indicates three measures of prediction accuracy: error rate, quadratic loss, and logarithmic loss. It also describes two types of counterproductive behavior that is having 5 different levels, ranging from the lowest (report low incidence) to the highest indicating (high incidence).

Moreover, Greitzer et al. [47] presented a description logics model for the psychological factors involved in identifying threats. The model involves various observable behaviors such as performance, stress, and confrontation. For each of the behaviors, there is a probability that approximates how frequently it occurs and how significant the behavior is to observing threats. However, as an observer is needed to measure whether the insider is exhibiting these behaviors, the assessment becomes subjective, which lacks reliability. A large number of ex-employers with a short average time spent with each activity may indicate unreliability. This can be detected from the background indicators [71]. Additionally, Brdiczka et al. [26] used psychological profiling regarding the Big-5 model involving social networks, behavioral, and word analysis as data for the profiling of

insider threats. However, the authors used gaming as their instrumentation, which has been criticized as not real data.

A sufficient insider threat monitoring and detection framework is needed for early prediction and detection of risk. Despite this, the insider threat problem continues. The application of these approaches to real-life environments seems to be a common theme among research. As such, to conduct profiling, insiders need to give consent; this is challenging as it requires specific ethical considerations that cannot be ignored. However, the criticality of insider threat has been highlighted throughout this section, and to develop further understanding, incorporating technical, behavioral, and psychological assessments are essential.

6. Open Problems and Future Directions

This section presents two key aspects: open problems and future directions related to insider threats.

6.1. Open Problems Related to the Insider Threat

Due to the inextricable link between human behavior and the combination of technical and non-technical aspects, providing a solution for insider threat for all organizations can be a multifarious problem. For example, understanding and mitigating insider threats can be complex due to the elements, such as outsourcing, globalization, and technological advances. These elements can blur the line between traditional insiders and external adversaries, such as terrorists who may conspire with physical insiders to access a system and its assets.

According to the Ponemon Institute survey of privileged users [72], one of the biggest challenges for companies is having difficulty knowing if an action delivered by an insider is a justifiable threat. It is hard to detect malicious actions unless we have imposed high standards of security policies and controls in place within an organization. Therefore, it is extremely important to revisit the security policy and control measures in place and add new rules and controls as per the need of the organization in order to detect and get alerted about the actions of its employees. The security tools they have, harvest too many false positives and do not produce enough contextual information. Moreover, high-tech tools including endpoint monitoring for detection are not widely used [72]. Therefore, there is a need of improving these tools or develop new tools in line with the current cyber security requirements.

The behavior involved in the insider threat incidents can be difficult to detect as the actions are consistent with the individual's role and responsibilities. Another problem is that organizations are finding that enforcing privileged user access rights is challenging. It is difficult to keep up with the amount of access change requests that occur regularly and the time it takes to deliver access to privileged users takes a long time [72]. Furthermore, 30% of privileged users state that within their organization, it is still too expensive to monitor and control all privileged users, which is still a concern. A new problem is that organizations are allowing users who have administrative or root-level access rights to work from home. This is problematic as keeping the data secure from the insider can be more challenging. Moreover, 41% of privileged users believe their organizations are not properly vetting background checks before receiving access rights. Therefore, there are still problems to be solved for organizations regarding the insider threat as the expansive nature of attacks can occur at any exploitation point within the company.

6.2. Future Directions for Addressing the Insider Threat Categories

This section highlights the future directions for addressing insider threats in different forms, targeting different subsystems of the organization.

6.2.1. Collaborative Insider Threat

Collaborative information systems (CISS) permit different groups of users to connect and collaborate over shared tasks. It is predicted that the greatest security threat to information systems

stems from insiders [54]. Several methods have been established to address the insider threat in collaborative settings. Formal access control frameworks are adapted to contextual scenarios. Knowing that access control is essential, but not adequate to promise safeguard, anomaly detection methods are proposed to detect deviations from the expected behavior. The access control mechanisms are the main protection method against insider threats [73]. Due to access control being broadly implemented in commercial information systems, databases, and software, it is overall successful in preventing insider attacks. However, more specialized attacks have been developed and circumvent security mechanisms. These attacks involve the collaboration of two or more insiders, which create challenging detection efforts. A model that is applicable to both single-step attacks and attacks with communication relays between insiders is helpful and a detection and collaborative approach will bridge data items. The transaction's distance to a data item can also support detecting malicious information that is created by the insiders.

Furthermore, the 2019 Insider Threat Report mentioned that the careless users cause most accidental breach (70%), while the users willfully ignoring policy (not malicious) and the users willfully causing harm are 66% and 62%, respectively, responsible for negligent and malicious data breaches [74]. The report emphasized that all teams and their members automatically adhere to company governance, compliance, and data-centric privacy and security policies upon creation. In such instances, a trust-based blockchain can be a good solution to protect the integrity of the information shared among the collaborative network peers, increasing their liability, and protecting their association by thwarting insider attacks [75]. Intrusion detection system (IDS) deployment can also become vulnerable to insider threats due to its interconnected and distributed nature [76]. An insider intruder can easily dominate any of the security nodes of the collaborative intrusion detection network and leave the entire security system vulnerable. Their work improves the insider attack detection accuracy by utilizing collaborative Snort node with blockchain certificates.

Overall, it is imperative to keep auditing the data—identify where all your data currently exist—both at rest and in motion. Especially, track carefully all access to sensitive data as well as actions.

6.2.2. Insider Threat on Personal Devices

Boral et al. [77] developed a diamond theory to counter insider threats on personal devices (such as laptops and flash drives) involving four methods of increasing the security of personal devices: software design, information retrieval, detection methods, and policy design. Based on past research and incidents, they argue that the diamond theory is an effective solution to mitigating risks to a company. However, the work does not explain how this would be used to identify malicious insiders or insider threats, but only introduces the four design characteristics of the diamond theory. Further, Majeed et al. [78] discussed a diverse perception of security and privacy concerns in the Internet of Everything (IoE) by establishing insiders carrying personal smart devices to use within the organization. Awareness to the employees about legal compliance and ethical compliance is crucial and it should be a requirement for adopting the ethical framework within an organization and provisioning training.

Moreover, security analysts of an organization need operative visual interfaces and interactive techniques that could detect security breaches and efficiently share threat information with the respective user or authority. A user behavior tool such as user behavior analytics (UBA) tool from IBM's security analytics environment can provide a rigorous data analysis [79]. This tool is quite effective in terms of conducting a continuous analysis of individuals' usage of their organizational IT networks and devices. This is a great way to effectively visualize the associated insider threats, security incidents, and associated data from various sources (e.g., HR systems) through a risk-focused dashboard, and aggregate risk levels associated with individual users, user groups, and overall system.

Overall, it is important to keep track of individual usage, data access, and data storage on personal devices.

6.2.3. Trusted Insiders Exploiting Personally Identifiable Information (PII)

Extensive research has been developed into various honeypot technologies, such as honeynets and honeytokens, to accumulate information on external threats [80]. Honeypots are trap systems or servers positioned within the network that attract targets for malicious users (such as insiders) and attackers. The honeytokens are fake digital data objects embedded among real data objects and utilized in exposing data misuse by insiders. However, it should be well investigated on how honeytokens can be implemented to catch insider threats. White and Panda [81] explored how honeytokens can be integrated to catch trusted insiders who want to exploit PII data. They found that by deploying internal PII honeytokens, they can be used as warning systems and they can detect prohibited behaviors before they have accelerated into detrimental data leaks. They can be deployed in numerous locations, such as the file space of the personal information and packets sent across the network. Further, Harilal et al. [82] collected a comprehensive dataset comprising interactive malicious insider threat instances involving both masqueraders and traitors. This was accomplished by building a gamified setting where the sales departments of competing companies (represented by groups) contacted a common set of customers. Unlike others, in this work, the malicious masquerader and traitor activities were performed by the actual users and not assumed to be injected into the dataset.

It is important to verify the feasibility of using physical movement logs gathered via a building access control system [83]. This consists of an understanding of the layout and assets of the building and detection method of malicious insider behavior. A systematic framework that uses contextual knowledge about the system and its users can be helpful here, which can learn from historical data gathered to offer a suitable model for real movement behavior. The effectiveness of this framework needs to be demonstrated by using real-time data traces of the user movement.

Overall, it is significant to restrict PII access and those who have access to PII must be monitored through their movement behavior and ask for the authentication.

6.2.4. Malicious Insiders in the Cloud Environment

Monitoring the patterns of malicious insiders who have access to a system is a noteworthy problem that is faced by providers in the Cloud environment. Although there are many benefits to Cloud users, there are some security issues. An insider threat detection model that uses sequential rule mining by associating incoming events against user profiles can be adopted [84]. Techniques such as machine learning algorithms and statistical modeling have been used to identify deviant user patterns in operating a system. Moreover, system calls can build profiles of malicious insiders in a system by using two methods: user-oriented model and process-oriented model [85]. For the user-oriented model, the access patterns are acquired to create meaningful data to build a pattern for a specific user. The process-oriented model controls how processes are used to access files in a system.

Moreover, an ontology-based framework for improving physical security and insider threat detection [86] can also be useful considering it supports threat detection using rule-based anomaly detection, forensic data analysis for attack attribution and thwarts deception, reconstructing complex attack patterns for enriching and sharing intelligence, as well as continuous security compliance monitoring. Live, network, and memory forensics are useful in detecting the footprint of insider threats. Live forensic is a process of analyzing digital evidence while the event is still in the process, which is the opposite of dead forensic. Network forensic is another area of digital forensic that deals with the analysis and investigation of network attacks. Memory forensic allows the analysis and retrieval of the data from the volatile memory that contains the current state of applications, operating system (OS), and application data. Digital evidence as the data (text, video, audio, and images) is processed and cached sometimes in a log file or transmitted with the support or disprove a theory of how the stealing of data occurred.

Overall, the user-oriented and process-oriented controls with rule-based anomaly detection and forensic data analysis are required for monitoring insider activities in the Cloud.

6.2.5. Corporate Insider Threat

A user and role-based profile with an anomaly detection system incorporating technical and behavioral activities are effective to be considered, which examines possible threats imposed by individuals [87]. Data from an activity log can be construed from the user and created into a tree-structured profile for the users and their associated roles. This activity allows a comparison between the users and their roles, whilst also providing an image representation of the present behavior of each user. This can then be compared with other observations and peer observations.

Traditional intrusion detection systems are not capable of identifying malicious insiders within an organization. In this direction, an automated system based on tree-structure profiling, which is capable of detecting insider threats within an organization, can be valuable [88]. Such a system incorporates activities details of each user and each job role and uses this data to deliver rich information about the user's actual behavior. The deviation can be measured based on the volume of variance that each user shows across multiple attributes compared to their peers.

Attribute-based access control (ABAC) is considered a promising alternative to the traditional models of access control (including, role-based access control (RBAC)), where possible, in the corporate and industrial context. ABAC and RBAC are effective ways of controlling the authentication process and authorizing users and their access rights. The key difference between ABAC and RBAC is that ABAC provides access rights centered on the user, environment, or resource attributes, whereas RBAC offers access to resources based on user roles. However, ABAC brings several unexplored issues such as audibility, scalability, hierarchical structure representations, delegation, and administration. Servos et al. [89] provided a comprehensive review of recent research efforts toward emerging the formal model of ABAC. The organizational data have been the most vulnerable to attacks by insiders, especially data located in databases and corporate file servers. Anomaly detection is a useful technique for alerting early marks of insider attacks, current techniques in database access are not much effective in detecting the sophisticated data misuse events (e.g., data updates track and the data aggregation) by the insiders [90]. Besides, monitoring the complete data retrieved by each user and comparing it to a base level result in low accuracy and long detection time. A detection technique for data aggregation that attempts to track data updates can also be adopted. Such a technique infers the regular rates of table references and tuples retrievals from past database access logs and analyzes user queries that lead to exceeding the normal data access rates.

Mostly unsupervised behavioral anomaly detection techniques are developed to find abnormal changes in user behavior over time. However, anomalous activities (temporal changes) are not necessarily malicious in nature. A time-series classification technique of user activities for insider threat detection is ideal to use as outperforms other traditional techniques based on unsupervised behavioral anomaly detection [91].

Overall, technical and behavioral activities along with data aggregation attempts to track data updates, and temporal changes are to be observed through activity logs and user profiles.

6.2.6. Insider Threat in Organizational IT Systems

The preventive measures need to be taken that assess the risks as well as reactive methods to combat the problem of insider threats [92]. In this direction, an identification-based framework is suitable for the initial requirement analysis of the organizational IT systems. Such a framework gives security engineers the support of detecting insider threats and presents prioritization dependent on the risk they pose to the organization. Within the requirement modeling language, an asset model and a trust model can also be considered, which permit the detection of insiders. The asset model associates the security properties and sensitivity levels to assets, whilst the trust model stipulates the trust level that a user puts into another user regarding permission on an asset. The one-class anomaly detection method can also be implemented, which measures classified resembles between the history of a user and events recorded in a time-window of the user's session [93]. This idea is based on the weighted oriented graph partitioning technique for event sequences where the strongly connected

nodes have to belong to the same cluster. Alternatively, a system based on a neural network with long short-term memory (LSTM) can be embraced, which simulates a system logs as a natural structured sequence and captures patterns of the users' normal usage behavior to distinguish normal behavior from malicious acts [94].

Overall, risk prioritization, security properties, and sensitivity levels to assets, identification-based, and similarity-based detection methods are required.

6.2.7. Combat Insider Threat in Enterprise Business

To combat insider threat, a combination of the enterprise business processes and the human factor is needed that inhibits them [95]. A process monitoring model is suitable to use that merges observing at the runtime level. The input involves psychometric evaluations from social media profiles of employees. The human factor aspect is considered as well as the technical approaches to monitoring. As its countermeasures, Homoliak et al. [12] identified five subcategories of the defense solutions: (a) mitigation and prevention, (b) detection and threat assessment, (c) best practices and guidelines, (d) decoy-based solutions, and (e) other practical solutions. Moreover, for a real demonstration, real insider threat data were collected from several host-based heterogeneous data sources (such as mouse, keyboard, processes, and file system) through a gamified process [82]. The users as investors can make a deal by spending some points they have and during masquerade sessions at specific intervals, each group was given access to the resource (a machine in this case) that belonged to another group. The whole idea is to allow stealing of the list of contacted investors from the victim's machine, and thus prevent other groups from winning. It demonstrates that combating insider threats in business through a gamified environment is quite effective.

Many real-world applications differ in their data collection techniques and dissimilarity in deployment environments. It can happen that one kind of machine learning-based detection system may not be effective and efficient for other systems. In such cases, methods that allow a previously trained population of linear genetic programming (LGP), an insider threat detector is useful to adapt to an expanded feature space [96]. This reduces the computation requirements and accelerating deployment under new conditions. Moreover, technology-based analysis is divided into two parts: host-based and network-based. A data source is generated from the insider's continuous interaction with the system (host). These interactions consist of application-level data, for example, keystrokes and mouse dynamics, Unix Syslog, windows event log, and operating system low-level data like data such as system calls. Window specific sensors can also be used to collect data from analytical system events such as key registry modification, system file operations, and process creation to create a biometric motivated solution to detect malignant insiders and deter impersonations. The network-based analysis includes data filtering and classification using machine learning, statistical analysis, and rule-based analytical techniques to determine the type of threat. All the servers (such as Dynamic Host Configuration Protocol—DHCP server, Lightweight Directory Access Protocol—LDAP server, web server, proxy, and email Server) deployed in the network are responsible for generating network logs.

Overall, a combination of the enterprise business processes and human factors can be used to detect malicious behavior. Additionally, psychometric evaluations from social media profiles of employees and the trained population-based threat detector are useful to consider.

6.2.8. Insider Threat via Social Engineering

Social engineering allows interaction between humans to extract entry information or unauthorized access for the system in an illegal way. Since not every staff member(s) is trained, they lack building confidentiality in handling such phishing campaigns. In addition to looking at the technical methods, an emotional way of thinking can be useful in understanding human nature to detect, say, the phishing email [97]. Two factors most influence human nature: personality and culture. Personality factors can be agreeableness, neuroticism, conscientiousness, extraversion, and openness to experience. The insiders do use these personality and cultural factors to target a phishing activity, hence, such factors can help to detect malicious or fake information.

A malicious insider may send or receive sensitive information as email images attachments. As a solution, the Email Attachments Receiver (EAR), which is a custom-built application, can be used to search Google Mail (Gmail) for images [98]. The application allows an analyst to comment on the image and investigate whether the image was previously seen, hence, decreasing false positives. However, a formal analysis of the images is necessary at a later stage as enhancements are needed, such as improvements in handling large datasets and postulating other analyst views.

One of the most critical challenges is to pinpoint and incorporate behavioral (sociotechnical) indicators of insider threat risks in addition to the common cyber and technical indicators. For that, it is important to consider readily available data. The insider threat techniques most often fail to address the human side issues. Greitzer et al. [99] performed a study with experts to complete email-based and online surveys and developed an inclusive insider threat ontology called, Sociotechnical and Organizational Factors for Insider Threat (SOFIT), which includes behavioral and organizational indicators as well as technical indicators. Their study was based on the threat ratings of single indicators, ratings for scenarios involving multiple indicators, temporal associations, and comparing fear with likelihood threat ratings.

Overall, the internal threat sensitivity of different personality characters is unclear and cultural differences of employees are not sufficiently appreciated and considered in research. The combination of the weighted personality, abilities, training and skills, dynamic emotions and attitudes, sociotechnical indicators, and culture can forecast individual and organizational undesirable and adverse impact behaviors.

7. Conclusions

In summary, insider threat is still a real challenge for organizations. This work has investigated insider threats and their criticality for organizations to combat these threats to mitigate risk. Malicious insiders have become a major security issue for all enterprises as insiders can range from low-level employees to high ranking personnel that have knowledge and access to confidential organizational information. Privilege escalation, exfiltration attacks, and APTs are some of the many techniques utilized by malicious insiders. To execute their attack, an insider needs to complete all stages of the kill chain, thus improving defenses at all phases of the kill chain can help deny future attacks. Improving defenses can be done through the establishment of sound security policies and monitoring of employee activity is essential in defending against malicious insider activity. Thus, the critical evaluation of the insider threat serves as a tool for organizations to expand their knowledge of this ever-evolving threat. As previously mentioned, different forms of insider threats need to be addressed (detect the threat and prevent any inappropriate access of organizational resources), which target different subsystems of the organization, such as device level, data level, and corporate and business level.

Author Contributions: N.S. and E.H. contributed to conceptualization and original draft writing, E.B. and N.S. contributed to investigation, methodologies, editing and revisions, P.O. contributed to the creation of tables and thoughts on indicators of compromise, K.-K.R.C. and P.B. contributed to resources, reviews and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Omar, M. Insider Threats: Detecting and Controlling. In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*; IGI Global: Hershey, PA, USA, 2015; p. 162.
2. Barrios, R.M. A multi-leveled approach to intrusion detection and the insider threat. *J. Inf. Secur*. **2013**, *4*, 54–65.
3. Cost of Insider Threats Global Report, Observer IT. 2020. Available online. https://www.observeit.com/cost-of-insider-threats (accessed on 25 Jun 2020).

4. ENISA Threat Landscape Report. 15 Top Cyber-Threats and Trends, Heraklion. European Union Agency for Network and Information Security (ENISA). 2016. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 (accessed on 27 Apr 2020).
5. ENISA Threat Landscape Report. 15 Top Cyber-Threats and Trends. Heraklion, European Union Agency for Network and Information Security (ENISA). 2018. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (accessed on 16 Jun 2020).
6. CPNI Insider Data Collection Study. London: Centre for the Protection of National Infrastructure. 2013. Available online: https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf (accessed on 25 Apr 2020).
7. Warkentin, M.; Willison, R. Behavioral and policy issues in information systems security: The insider threat. *Eur. J. Inf. Syst.* **2009**, *18*, 101–112.
8. Yang, S.C.; Wang, Y.L. Insider threat analysis of case based system dynamics. *Adv. Comput. Int. J. ACIJ* **2011**, 2, 1–17.
9. Trzeciak, R.F. SEI Cyber Minute: Insider Threats. 2017. Available online: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496626 (accessed on 15 Jun 2020).
10. Insider Threats Survey, April 2011. Available online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/31/2011/07/07061213/insider_threats_survey.pdf (accessed on 7 Jun 2002).
11. Liu, L.; de Vel, O.; Han, Q.; Zhang, J.; Xiang, Y. Detecting and preventing cyber insider threats: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1397–1417, doi:10.1109/COMST.2018.2800740.
12. Homoliak, I.; Toffalini, F.; Guarnizo, J.; Elovici, Y.; Ochoa, M. Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Comput. Surv.* **2019**, *52*, doi:10.1145/3303771.
13. Gheyas, I.A.; Ali, E.A. Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Anal.* **2016**, *1*, 1–29.
14. Cappelli, D.M.; Moore, A.P.; Trzeciak, R.F. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley. Available online: http://ptgmedia.pearsoncmg.com/images/9780321812575/samplepages/9780321812575.pdf (accessed on 27 May 2020).
15. Insider Threat, Imperva. Available online: https://www.imperva.com/learn/application-security/insider-threats (accessed on 7 May 2020).
16. Compromised Insider, The Problems It Causes Organisations?, Cyberseer. Available online: https://www.cyberseer.net/solutions-and-services/common-threats/compromise-insider (accessed on 18 Jun 2020).
17. L. Ponemon. Cost of data breach study: Global analysis. Poneomon Institute sponsored by Symantec. 2013. Available online: https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf (accessed on 3 Jun 2020).
18. Categories of Insider Threats. Intelligence and National Security Alliance (INSA). 2019. Available online: https://www.insaonline.org/wp-content/uploads/2019/ 10/INSA_WP_Categories_of_Insider_Threats-1.pdf (accessed on 13 Jun 2020).
19. Moore, A.P.; Cappelli, D.M.; Caron, T.C.; Shaw, E.; Spooner, D.; Trzeciak, R.F. A preliminary Model of Insider Theft of Intellectual Property (No. MU/SEI-2011-TN-013). Carnegie-Mellon Univ Software Engineering Inst, USA, 2011. Available online: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2011_004_001_15362.pdf (accessed on 5 Jun 2020).
20. Greitzer, F.L.; Strozer, J.; Cohen, S.; Bergey, J.; Cowley, J.; Moore, A.; Mundie, D. Unintentional insider threat: Contributing factors, observables, and mitigation strategies. In *Proceedings of the 47th Hawaii International Conference on System Sciences*, Waikoloa, HI, USA, 6–9 January 2014; pp. 2025–2034.
21. White, S.J. Assessing Cyber Threats and Solutions for Municipalities. In *Cyber-Physical Security*; Springer: New York, NY, USA, 2017; pp. 49–65.
22. Nurse, J.R.; Buckley, O.; Legg, P.A.; Goldsmith, M.; Creese, S.; Wright, G.R.; Whitty, M. Understanding insider threat: A framework for characterising attacks. In *Proceedings of the 2014 IEEE International Symposium on Security and Privacy Workshops (SPW)*, San Jose, CA, USA, 17–18 May 2014; pp. 214–228.
23. Cassidy, T. Workplace Violence and Insider Threat. 2018. Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=525011 (accessed on 1 Jun 2020).

24. J. Umawing. Workplace violence: The forgotten insider threat. 2018. Available online: https://blog.malwarebytes.com/101/2018/10/workplace-violence-the-forgotten-insider-threat (accessed on 30 May 2020).
25. Haggard, S.; Lindsay, J.R. *North Korea and the Sony Hack: Exporting Instability Through Cyberspace*; AsiaPacific Issues 117; East-West Center: Honoloulu, HI, USA, 2015; pp. 1–8.
26. Gupta, S.; Kumar, P. Taxonomy of cloud security. *Int. J. Comput. Sci. Eng. Appl.* **2013**, *3*, 47–52.
27. Jaafar, F.; Nicolescu, G.; Richard, C. A systematic approach for privilege escalation prevention. In *Proceedings of the IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Vienna, Austria, 1–3 August 2016*; IEEE: New York, NY, USA, 2016; pp. 101–108.
28. Tsoutsos, N.G.; Maniatakos, M. Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation. *IEEE Trans. Emerg. Top. Comput.* **2014**, *2*, pp. 81–93.
29. Janssen, C. Data Exfiltration. Techopedia. 2015. Available online: http://www.techopedia.com/definition/14682/data-exfiltration (accessed on 28 Apr 2020).
30. Giani, A.; Berk, V.H.; Cybenko, G.V. Data exfiltration and covert channels. *Proc. SPIE* **2006**, *6201*, doi:10.1117/12.670123.
31. Clark, J.; Leblanc, S.; Knight, S. Risks associated with USB hardware Trojan devices used by insiders. In *Proceedings of the IEEE International Conference on Systems Conference (SysCon)*, Montreal, QC, Canada, 4–7 April 2011; pp. 201–208.
32. Cleghorn, L. Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth. *J. Inf. Secur.* **2013**, *4*, 144–149.
33. Pernet, C. AIRBUS, APT Kill Chain—Part 3: Reconnaissance. 2014. Available online: https://airbus-cyber-security.com/apt-kill-chain-part-3-reconnaissance (accessed on 30 Apr 2020).
34. Gates, S. Threat Intelligence Predictions Report, NSFOCUS 2017. Available online: http://blog.nsfocusglobal.com/wp-content/uploads/2017/02/TI-2017_Predictions_Report__v4.pdf. (accessed on 2 May 2020).
35. Harrysson, M.; Metayer, E.; Sarrazin, H. How social intelligence can guide decisions. *McKinsey Q.* **2012**, *4*, 81–89.
36. Shullich, R. Risk Assessment of Social Media. The SANS Institute USA. 2012. Available online: https://www.sans.org/reading-room/whitepapers/riskmanagement/paper/33940 (accessed on 7 May 2020).
37. Giura, P.; Wang, W. A context-based detection framework for advanced persistent threats. In *Proceeding of the 2012 International Conference on Cyber Security (CyberSecurity)*, Washington, DC, USA, 14–16 December 2012; pp. 69–74.
38. Potts, M. Lancope. Internal Network Visibility for APTs and Insider Threats. Alpharetta: Lancope, Inc. 2016. Available online: https://www.insightssuccess.com/lancope-preeminent-network-visibility-and-security-intelligence/ (accessed on 15 May 2020).
39. Hutchins, E.M.; Cloppert, M.J.; Amin, R.M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington, DC, USA, 16–18 March 2011; pp. 80–81.
40. Ray, L.; Felch, H. Detecting advanced persistent threats in oracle databases: Methods and techniques. In *Strategic Information Systems and Technologies in Modern Organizations*; IGI Global: Hershey, PA, USA, 2017; pp. 71–89.
41. Scott, J.; Spaniel, D. In 2017, The Insider Threat Epidemic Begins. Institute for Critical Infrastructure Technology. February 2017. Available online: https://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In-2017-The-Insider-Threat-Epidemic-Begins.pdf (accessed on 14 Jun 2020).
42. Kuo, J. Data Reconnaissance and Injection. Ph.D. Thesis, California State Polytechnic University, Pomona, CA, USA, 2017.
43. Olavsrud, T. 11 Steps Attackers Took to Crack Target. 2014. Available online: https://www.cio.com/article/2600345/11-steps-attackers-took-to-crack-target.html (accessed on 18 May 2020).
44. A Kill Chain Analysis of the 2013 Target Data Breach. Committee on Commerce, Science and Transportation. 2014. Available online: https://www.omegasecure.com/wp-content/uploads/2016/03/Target_Kill_Chain_Analysis_FINAL-1.pdf (accessed on 21 May 2020).
45. CERT. Common Sense Guide to Mitigating Insider Threats, 4th Edition, United States, Carnegie Mellon Software Engineering Institute. 2012. Available online:

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf (accessed on 22 May 2020).

46. Shaw, E.D.; Stock, H.V. *Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall*; White Paper; Symantec: Mountain View, CA, USA, 2011.
47. Greitzer, F.L.; Hohimer, R.E. Modeling human behavior to anticipate insider attacks. *J. Strateg. Secur.* **2011**, *4*, 25–26.
48. Hunker, J.; Probst, C.W. Insiders and insider threats-an overview of definitions and mitigation techniques. *J. Wirel. Mob. Netw. Ubiquitous Comput. Depend. Appl.* **2011**, *2*, 4–27.
49. Oracle Database Vault. 2015. Available online: https://www.oracle.com/technetwork/database/security/database-vault-ds-12c-1898877.pdf (accessed on).
50. Iyer, R.; Dabrowski, P.; Nakka, N.; Kalbarczyck, Z. Pre-configurable tamper-resistant hardware support against insider threats: The tested ILLIAC approach. In *Insider Attack and Cyber Security*; Springer: New York, NY, USA, 2008, pp. 133–152.
51. Kumar, G.P.; Morarjee, K. Ranking prediction for cloud services from the past usages. *Int. J. Sci. Eng.* **2014**, *2*, pp. 22–25.
52. Mihai, I.-C.; Pruna, S.; Barbu, I.-D. Cyber kill chain analysis. *Int. J. Inf. Secur. Cybercrime* **2014**, *3*, 37–42.
53. Greitzer, F.L.; Strozer, J.R.; Cohen, S.; Moore, A.P.; Mundie, D.; Cowley, J. Analysis of unintentional insider threats deriving from social engineering exploits. In *Proceedings of the IEEE Security and Privacy Workshops*, San Jose, CA, USA, 17–18 May 2014; pp. 236–250, doi:10.1109/SPW.2014.39.
54. Chen, Y.; Nyemba, S.; Malin, B. Detecting anomalous insiders in collaborative information systems. *IEEE Tran. Dependable Secur. Comput.* **2012**, *9*, 332–344.
55. Gordon, L.A.; Loeb, M.P.; Zhou, L. Investing in cybersecurity: Insights from the gordon-loeb model. *J. Inf Secur.* **2016**, *7*, 49–59.
56. Microsoft Are Your Insiders Really Who You Think They Are? NetIQ Corporation. 2007. Available online: https://www.netiq.com/docrep/documents/h4mylk7uec /netiq_pb_group_policy_admin.pdf (accessed on 25 May 2020).
57. CERT. Insider Threat Control: Using a SIEM signature to detect potential precursors to IT Sabotage. Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213. Available online: https://insights.sei.cmu.edu/insider-threat/2012/01/insider-threat-control-using-a-siem-signature-to-detect-potential-precursors-to-it-sabotage.html (accessed on 13 Jun 2020).
58. Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access* **2018**, *6*, 25167–25177, doi:10.1109/ACCESS.2018.2817560.
59. Turner, J.T.; Gelles, M. Threat assessment: A risk management approach. Routledge, 2012. Available online: https://www.tandfonline.com/doi/abs/10.1080/00029157.2009.10401683 (accessed on 7 Jun 2020).
60. Brdiczka, O.; Liu, J.; Price, B.; Shen, J.; Patil, A.; Chow, R.; Bart, E.; Ducheneaut, N. Proactive insider threat detection through graph learning and psychological context. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, 24–25 May 2012; pp. 142–149.
61. Cassidy, T. Technical Detection of Intended Violence: Workplace Violence as an Insider Threat. 2017. Available online: https://insights.sei.cmu.edu/sei_blog/2017/12/technical-detection-of-intended-violence-workplace-violence-as-an-insider-threat.html (accessed on 12 Jun 2020).
62. The global state of information security, PWC, 2014. Available online: http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml (accessed on 10 Jun 2020).
63. Security of Cloud Computing Providers Study. Ponemon Institute, LLC. 2011. Available online: http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computingproviders-final-april-2011.pdf (accessed on 11 Jun 2020).
64. Rashid, T.; Agrafiotis, I.; Nurse, J.R.C. A new take on detecting insider threats: Exploring the use of hidden Markov models. In *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, Vienna Austria, 28 October 2016; pp. 47–56.
65. Yates, D.; Harris, A. International Ethical Attitudes and Behaviors: Implications for Organizational Information Security Policy. In: *Information Assurance and Security Ethics in Complex. Systems: Interdisciplinary Perspectives*; IGI Global: Hershley, PA, USA, 2011; pp. 55–80.

66. Greitzer, F.L.; Frincke, D.A.; Zabriskie, M. Social/ethical issues in predictive insider threat monitoring. In *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*; IGI Global: Hershey, PA, USA, 2010; pp. 132–161.
67. Swiety, M. From Ethics to Insider Threats: How Can You Protect Your Business?. 2018. Available online: https://www.luxoft.com/blog/mswiety/from-ethics-to-insider-threats-how-can-you-protect-your-business (accessed on 25 Jun 2020).
68. Salem, M.B.; Hershkop, S.; Stolfo, S.J. A survey of insider attack detection research. In *Insider Attack and Cyber Security*; Springer: New York, NY, USA, 2008; pp. 69–90.
69. Hashem, Y.; Takabi, H.; GhasemiGol, M.; Dantu, R. Inside the mind of the insider: Towards insider threat detection using psychophysiological signals. *J. Internet Serv. Inf. Secur.* **2016**, *6*, 20–36.
70. Axelrad, E.T.; Sticha, P.J.; Brdiczka, O. A bayesian network model for predicting insider threats. In *Proceedings of the IEEE Security and Privacy Workshops*, San Francisco, CA, USA, 23–24 May 2013; pp. 82–89.
71. Kont, M.; Pihelgas, M.; Wojtkowiak, J.; Trinberg, L.; Osula, A.-M. Insider Threat Detection Study. NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). 2014. Available online: https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf (accessed on 14 Jun 2020).
72. Privileged User Abuse & The Insider Threat. Ponemon Institute Research Report. May 2014. Available online: http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/ content/rtn_257010.pdf accessed on 11 Jun 2020).
73. Viet, K.; Panda, B.; Hu, Y. Detecting collaborative insider attacks in information systems. In *Proceedings of the 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Seoul, Korea, 14–17 October 2012; pp. 502–507.
74. Bray, R.; Marsh, S. How to Secure Collaboration from Insider Threats. 2019. Available online: https://www.mesalliance.org/wp-content/uploads/2019/04/How-to-Secure-Collaboration-from-Insider-Threats-LiveTiles.pdf (accessed on 15 Jun 2020).
75. Kolokotronis, N.; Brotsis, S.; Germanos, G.; Vassilakis, C.; Shiaeles, S. On blockchain architectures for trust-based collaborative intrusion detection. In *Proceedings of the IEEE World Congress on Services (SERVICES)*, Milan, Italy, 8–13 July 2019; pp. 21–28, doi:10.1109/SERVICES.2019.00019.
76. Ujjan, R.M.A.; Pervez, Z.; Dahal, K. Snort based collaborative intrusion detection system using blockchain in SDN. In *Proceedings of the 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, Island of Ulkulhas, Maldives, 26–28 August 2019; pp. 1–8, doi:10.1109/SKIMA47702.2019.8982413.
77. Boral, L.; Disla, M.; Patil, S.; Williams, J.; Park, J.S. Countering insider threats in personal devices. In *Proceedings of the IEEE 2017 Intelligence and Security Informatics*, New Brunswick, NJ, USA, 23–24 May 2007; pp. 365–365.
78. Majeed, A.; Haq, A.U.; Jamal, A.; Bhana, R.; Banigo, F.; Baadel, S. Internet of everything (IoE) exploiting organisational inside threats: Global network of smart devices (GNSD). In *Proceedings of the IEEE International Symposium on Systems Engineering (ISSE)*, Edinburgh, UK, 3–5 October 2016; pp. 1–7, doi:10.1109/SysEng.2016.7753152.
79. Haim, B.; Menahem, E.; Wolfsthal, Y.; Meenan, C. Visualizing insider threats: An effective interface for security analytics. In *Proceedings of the 22nd ACM International Conference on Intelligent User Interfaces Companion (IUI Companion)*, Limassol, Cyprus, 13–16 March 2017; pp. 39–42.
80. Shabtai, A.; Bercovitch, M.; Rokach, L.; Gal, Y.; Elovici, Y.; Shmueli, E. Behavioral Study of Users When Interacting with Active Honeytokens. *ACM Trans. Inf. Syst. Secur*. **2016**, *18*, doi:10.1145/2854152.
81. White, J.; Panda, B. Implementing PII honeytokens to mitigate against the threat of malicous insiders. In *Proceedings of the 2009 IEEE International Conference on Intelligence and Security Informatics*, Dallas, TX, USA, 8–11 June 2009; pp. 233–239.
82. A. Harilal; F. Toffalini; I. Homoliak; J. Castellanos; J. Guarnizo; S. Mondal. The wolf of SUTD (TWOS): A dataset of malicious insider threat behavior based on a gamified competition. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2018**, *9*, 54–85.
83. Cheh, C.; Thakore, U.; Fawaz, A.; Chen, B.; Temple, W.G.; Sanders, W.H. Data-driven model-based detection of malicious insiders via physical access logs. *ACM Trans. Model. Comput. Simul.* **2019**, *29*, doi:10.1145/3309540.
84. Nkosi, L.; Tarwireyi, P.; Adigun, M.O. Insider threat detection model for the cloud. In Proceedings of the 2013 Information Security for South Africa, Johannesburg, South Africa, 14–16 August 2013; pp. 1–8.

85. Nguyen, N.; Reiher, P.; Kuenning, G.H. Detecting insider threats by monitoring system call activity. In *Proceedings of the IEEE Systems, Man and Cybernetics Information Assurance Workshop*, West Point, NY, USA, 18–20 June 2003; pp. 45–52.
86. Mavroeidis, V.; Vishi, K.; Jøsang, A. A framework for data-driven physical security and insider threat detection. In *Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, Barcelona, Spain, 28–31 August 2018; pp. 1108–1115.
87. Legg, P.A.; Buckley, O.; Goldsmith, M.; Creese, S. Caught in the act of an insider attack: Detection and assessment of insider threat. In *Proceedings of the 2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, USA, 14–16 April 2015; pp. 1–6.
88. Legg, P.A.; Buckley, O.; Goldsmith, M.; Creese, S. Automated insider threat detection system using user and rolebased profile assessment. *IEEE Syst. J.* **2017**,*11*, 503–512.
89. Servos, D.; Osborn, S.L. Current research and open problems in attribute-based access control. *ACM Comput. Surv.* **2017**, *4*, doi:10.1145/3007204.
90. Sallam, A.; Bertino, E. Result-based detection of insider threats to relational databases. In *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY)*, Richardson, TX, USA, 25–27 March 2019; pp. 133–143.
91. Chattopadhyay, P.; Wang, L.; Tan, Y. Scenario-based insider threat detection from cyber activities. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 660–675.
92. Moyano, F.; Fernandez-Gago, C.; Paci, F. Detecting insider threats: A trust-aware framework. In *Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES)*, Regensburg, Germany, 2–6 September 2013; pp. 121–130.
93. Toffalini, F.; Homoliak, I.; Harilal, A.; Binder, A.; Ochoa, M. Detection of masqueraders based on graph partitioning of file system access events. In *Proceedings of the IEEE Security and Privacy Workshops*, San Francisco, CA, USA, 24 May 2018; pp. 217–227.
94. Lu, J.; Wong, R.K. Insider threat detection with long short-term memory. In *Proceedings of the ACM Australasian Computer Science Week Multiconference (ACSW)*, Sydney, Australia, 29–31 January 2019; pp. 1–10.
95. Gritzalis, D.; Stavrou, V.; Kandias, M.; Stergiopoulos, G. Insider threat: Enhancing BPM through social media. In *Proceedings of the 6th International Conference on New Technologies, Mobility and Security (NTMS)*, Dubai, United Arab Emirates, 30 March–2 April 2014; pp. 1–6.
96. Le, D.C.; Heywood, M.I.; Zincir-Heywood, N. Benchmarking genetic programming in dynamic insider threat detection. In *Proceedings of the ACM Genetic and Evolutionary Computation Conference Companion (GECCO)*, Kyoto, Japan, 15–19 July 2018; pp. 385–386.
97. Xiangyu, L.; Qiuyang, L.; Chandel, S. Social engineering and insider threats. In *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Nanjing, China, 12–14 October 2017; pp. 25–34.
98. Clark, J.W. EAR: An e-mail attachment receiver to search concerning images in the context of insider threat. In *Proceedings of the 40th IEEE Annual Computer Software and Applications Conference (COMPSAC)*, Atlanta, GA, USA, 10–14 June 2016; pp. 365–370.
99. Greitzer, F.L. Insider threats: it's the human, stupid!. In *Proceedings of the ACM Northwest Cybersecurity Symposium (NCS)*, Richland, WA, USA, 8–10 April 2019; pp. 1–8.