EAI Endorsed Transactions
on Security and Safety
Research Article EAI.EU

SoK: The Psychology of Insider Threats

Mubashrah Saddiqa[1],*, Jukka Ruohonen[1]

[1]The Maersk Mc-Kinney Moller Institute, University of Southern Denmark (SDU)

Abstract

This paper presents a systematic literature review on the psychology of insider threats—security risks originating from individuals within organizations. While this is a well-established research area, psychological perspectives remain underdeveloped. The extended version adds background to better contextualize the role of personality traits, psychological states, and situational factors in insider threats. The paper also highlights research gaps and the need for stronger theoretical foundations in this domain.

Keywords: cybercrime, organizational security, security incident, inside job, deterrence, personality traits, dark traits, systematic literature review

Received on 12 May 2025, accepted on 18 June 2025, published on 19 June 2025

doi: 10.4108/eetss.v9i1.9298

1. Introduction

Insider threats refer to perceived or real threats that come from people inside organizations[1]. These people, the insiders, such as employees and contractors, have inside information about an organization's security policies and practices, including cybersecurity measures. Due to their work, they also have legitimate access to organizations' information systems, computer networks, and other information technology infrastructures. Therefore, insider threats are particularly difficult to detect and prevent. If an insider threat is realized, the consequences may include theft of confidential or even classified information, theft of intellectual property and trade secrets, sabotage of information systems, or more general fraud. Despite such serious consequences, insider threats have been common throughout the world. According to some industry reports, even more than half of all cyber-attacks have been conducted by insiders [2]. As discussed, such numbers may be partially explained by the collusion between insiders and external threats, as is the case with phishing. Thus, other studies indicate smaller numbers. For instance, according to media sources, about ten percent of all data breaches have involved insiders [3]. Whatever the actual numbers may be, it can be concluded that insiders pose a significant threat to most organizations. That said, the issue is nontrivial and problematic because insiders are also a valuable asset to organizations. No organization can function without people.

Before continuing any further, it should be understood that the research on insider threats has been strongly divided between technical and non-technical research approaches [4]. The technical branch of research has focused on different profiling and anomaly detection techniques for computer use and network traffic. Thus, this branch aligns with the nowadays popular zero trust security model, which assumes that a part of an organization's technological infrastructure has already been compromised; therefore, logging, profiling, fine-grained access controls, and other related techniques should be applied [5]. Some studies have also connected technical profiling to insiders' cognitive styles [6], but such bridge-building studies have been rare. In contrast, the non-technical breach of research has focused on human behavior within organizations, often drawing from sociology, criminology, and related social science fields. Also, psychology has been a common reference field.

The divide in the research has also caused some schisms. While some authors have argued that the non-technical

* Corresponding author. Email: msad@mmmi.sdu.dk

[1] The paper is an extended version of an earlier conference paper [1]

branch has often been downplayed [7, 8], others have argued for a balanced approach that takes both technical and non-technical factors into account [9]. For the present purposes, it is important to emphasize that the non-technical research branch is generally less known than the technical branch of research.

Therefore, this paper presents a systematization of knowledge (SoK) in the form of a systematic literature review on the psychology of insider threats. While there are existing systematic literature reviews [10], as well as more general review articles [11], the systematization of existing knowledge is still limited, particularly with respect to psychology. The paper's contribution is thus clear and welcome.

In what follows, the paper proceeds in a straightforward manner: the background and context of insider threats, particularly from a psychological perspective, are discussed in Section 2, the methodology for the systematic literature review is addressed in Section 3, the results of the review are presented in Section 4, and the conclusion follows in the final Section 5. As discussed in the opening section, out of necessity, the review does not rely on quantification or related systematization techniques but instead concentrates on pinpointing relevant insights and gaps in the existing knowledge. The gaps and associated problems provide good opportunities for further research, as elaborated in the concluding section.

2. Background

Insider threats remain a substantial challenge for organizations due to the complex interaction of technical, psychological, and organizational factors [12]. While technical methods for detection and prevention are necessary, it is often claimed that understanding the psychological motivations behind insider behavior may also play a role. Insider threats are particularly challenging to detect and prevent because these individuals are often authorized to interact with organizational assets, making their activities less likely to raise suspicion. The psychological aspects of insider threats are frequently discussed in literature, although they represent a dimension that remains loosely defined and lacks consistent empirical validation. While much of the literature [13–15] has focused on technical approaches, some authors have argued that understanding the psychological and behavioral motivations of insiders could contribute to effective prevention and detection [16]. Psychological factors such as personal grievances, stress, and financial pressures are often cited as potential influences on an insider's likelihood of engaging in harmful activities, although again, robust theoretical models and replicable findings remain limited.

A key challenge in addressing insider threats is the dual role insiders play within organizations: they are both valuable assets and potential risks. No organization can function without people, and at the same time, insiders have wide opportunities to cause damage. Some research suggests a deeper understanding of the psychological profiles and motivations that drive individuals to breach organizational security [17]. One often cited example is the case of Edward Snowden [18], a former contractor for the National Security Agency (NSA). He had access to highly classified documents and disclosed a vast array of secret surveillance programs to the press, arguing that the public had a right to know about government surveillance activities. This case is frequently interpreted as an instance where personal beliefs and grievances may have contributed to the decision to leak classified information. While some view Snowden as a whistleblower [19], his actions are also seen as an illustration of how insiders can exploit their access based on personal or ideological motives. However, the broader applicability of such individual cases remains uncertain, and the psychological mechanisms underlying these decisions are not yet fully understood.

Some authors also argue that employees who feel undervalued, unsupported, or unfairly treated within their organization may be more likely to engage in malicious behavior as a form of retribution or self-justification [20, 21], though these claims often rely on theoretical models that have not been rigorously tested. In such narratives, insiders may rationalize their actions, viewing them as deserved or necessary due to perceived inequities or frustrations [22]. These kinds of psychological mechanisms are often proposed as explanations, but their predictive power and empirical basis are still debated.

Personality traits and cognitive biases are also frequently mentioned in discussions about insider threat risk. Traits [23] such as narcissism, Machiavellianism, or low empathy are hypothesized to increase the likelihood of self-interested behavior, potentially making individuals more prone to overlook the harm caused to the organization or colleagues. Similarly, cognitive biases [24], such as the normalization of deviance, are believed to contribute to gradual risk escalation, though again, these ideas are largely conceptual and not grounded in a unified or validated psychological framework.

Another key psychological factor in the development of insider threats is the role of organizational culture [25]. Trust, or the lack thereof, within an organization is sometimes alleged to contribute to an insider's decision to engage in harmful behavior. A toxic or distrustful work environment is said to raise resentment and disengagement, increasing the likelihood that insiders will act in ways that undermine the organization's security. On the other hand, a positive organizational culture that emphasizes open communication, fairness, and support is claimed to reduce the risk of insider threats by encouraging employees to feel valued and loyal to the organization [26]. As an example, a former Goldman Sachs employee [27] was convicted of stealing proprietary information, including trading algorithms and strategies, after expressing dissatisfaction with his employer. In this case, the employee felt that the company's treatment of him and his colleagues had contributed to a toxic work environment. While this case is commonly cited as an example that may illustrate the role

organizational culture might play, it remains largely an anecdotal example.

At the organizational level [28], leadership is frequently identified as an important influence on insider behavior. Leaders who model ethical conduct and communicate transparently are said to foster trust and share responsibility. In contrast, weak leadership and unclear ethical standards are sometimes associated with environments where insider threats are more likely to occur. However, much of this reason remains speculative and underexamined in empirical studies.

As discussed in the introduction, the research on insider threats has often been divided between technical and non-technical approaches. Technical research typically focuses on detection methods, such as monitoring network traffic, profiling users, or implementing zero-trust security frameworks. While these approaches are central to identifying threats in real time, they do not fully address the psychological and social dynamics that are sometimes claimed to underline insider behavior. In contrast, non-technical research, including perspectives from psychology, criminology, and sociology, attempts to explore the human factors that may contribute to insider threats. It examines how traits, culture, and behavioral patterns might play a role, though the conclusions drawn in this domain often lack rigorous testing or widespread consensus. As a result, these psychological perspectives remain underutilized in comparison to more established technical solutions.

This research explores the gap caused by the lack of integration between the technical and psychological aspects of insider threat studies. Through a systematic literature review, this paper aims to fill this gap by examining psychological insights related to insider threats.

3. Methodology

Conventional guidelines were followed for the systematic literature review; a protocol was specified prior to the literature search and only well-known databases were used to retrieve peer reviewed scientific papers [29]. Eight academic databases were queried, including the major ones in computer science: ACM Digital Library, IEEE Xplore, Springer Link, and ScienceDirect. Otherwise, the search was kept simple; auxiliary techniques [30] were thus omitted. For instance, bibliometric details (such as citations or impact factors) were not considered, and the search was not extended toward papers cited in the papers obtained from the database queries. The following query string was used to retrieve the search results from each database on June 10, 2024:

(insider AND threat AND psychology) OR
(insider AND threat AND psychological)

The search was limited to abstracts for all databases except Springer Link, which does not allow specifying the search location. For this database, the search term "insider threat", as specified in quotation marks, was used together with the terms psychology and psychological, as specified above. In addition, searches were restricted to conventional articles in journals and conference proceedings, such that book chapters and related content were excluded. As can be seen from Fig. 1, in total nearly 150 papers were returned by the searches. This large amount was reduced by qualifying only scientific papers, such that editorials and related content were excluded, which dealt with insider threats and psychology in the main body of the papers' text. This exclusion criterion implied that those papers were excluded that only dealt with the subject matter in terms of literature references, for instance. The final sample for the literature review contains n = 82 peer-reviewed papers. Most of these are computer science papers. Unlike what was expected prior to the searches, only a few relevant social science papers were retrieved. Moreover, HeinOnline, a major search portal for legal research, did not return a single paper.

The search procedure satisfies two of the desired properties of systematic literature reviews; the procedure was structured, and it is transparent. However, the third desired criterion, comprehensiveness, is not perfectly fulfilled because, particularly, the restriction to abstracts may have excluded some relevant papers. Even with this restriction, the number of papers is still much larger than in previous systematic literature reviews (n = 37) [10]. Furthermore, while some authors have maintained that all research addressing a specific question should be included [29], others have been less strict, arguing that all relevant research should be covered [31].

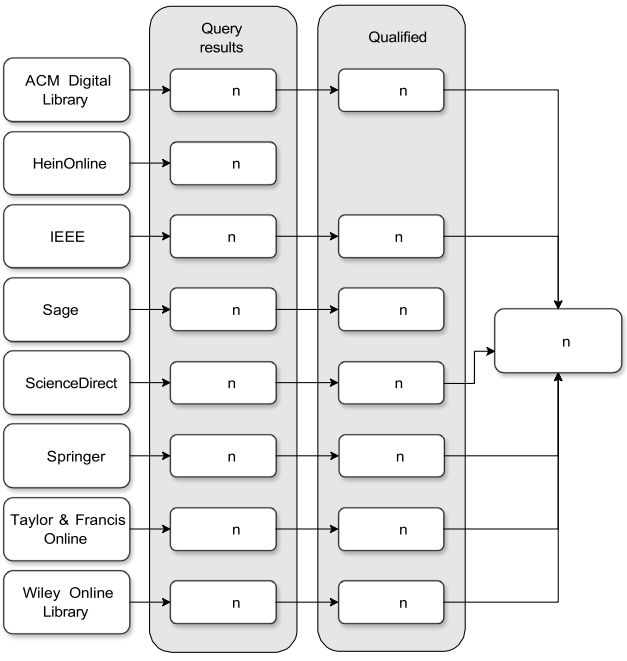

Figure 1. The Literature Search

In terms of relevance, the sample can be argued to be sufficient for addressing the existing knowledge about the psychology of insider threats—even if some papers are missing. As will be seen, existing knowledge is still fairly

immature, and this overall picture of immaturity would not likely change with a few more articles added to the review. Therefore, it could also be said that the paper is a systematic mapping study instead of a systematic literature review per se. In general, systematic mapping studies focus on thematic analysis, identifying relevant insights and research gaps, while the latter focuses on systematizing existing evidence [32]. Due to various different theories, variables, methods, and datasets, the insider threat literature is unfortunately too diverse for deducing actual evidence in the form of a meta-analysis or some other quantitative review technique.

4. Results

4.1. Taxonomies

Many of the papers presented or dealt with different taxonomies for insider threats. Because these taxonomies are to some extent related to psychology, it is helpful to consider some examples from literature. The examples also help at a high-level analytical framing of the literature.

Thus, the taxonomies typically separate intentional and unintentional insider threats and incidents [16, 33, 34]. The actual labels used tend to vary slightly from one, study to another but the same theme is still present; the same separation can thus also be referred to with the terms malicious and non-malicious [11, 35, 36]. What separates the two is intention; a malicious insider intends to compromise an organization for some goals, whereas non-malicious insiders may unintentionally compromise the organization with accidental or negligent but well-meaning mistakes or errors. With this basic separation at hand, it is possible to continue to further insider types. For instance, accidental insiders have no intent to cause harm, negligent and mischievous insiders cause harm but have no malicious intent, and purely malicious insiders cause deliberate harm for plain malice or other goals [16]. A further option is to consider incidental and deliberate harms. Then, whistleblowers may be seen to cause incidental harm for some societal goals and misbehavers for some personal reasons, whereas malicious insiders cause deliberate harm together with ideologues who have some political ideals and goals thereto [37]. This taxonomy is illustrated in Fig. 2, which further operates with an awareness of organizations' security controls and compliance procedures.

With respect to computer science research in particular, relevant is also the collusion between internal and external threats. According to the literature, a typical example would be social engineering with which external threat actors lure insiders to compromise an organization or parts of it. The example is relevant in terms of psychology research because it pinpoints toward analyzing the psychological vulnerabilities of insiders together with the psychological persuasion and manipulation techniques of external threat actors [38].

In terms of taxonomies, on the other hand, the collusion leads to further typologies, such as pure insiders, insider associates (such as contractors, security guards, or cleaners), inside affiliates (such as spouses, friends, or clients), and outside affiliates, including former employees [7]. Literature has also considered other types of a collusion. For instance, a concept of "cyber friendly fire" has been used to describe situations in which intentional security operations intended to protect an organization cause unintentional harms to the organization's security [35]. Another question is the usefulness of the taxonomies to begin with.

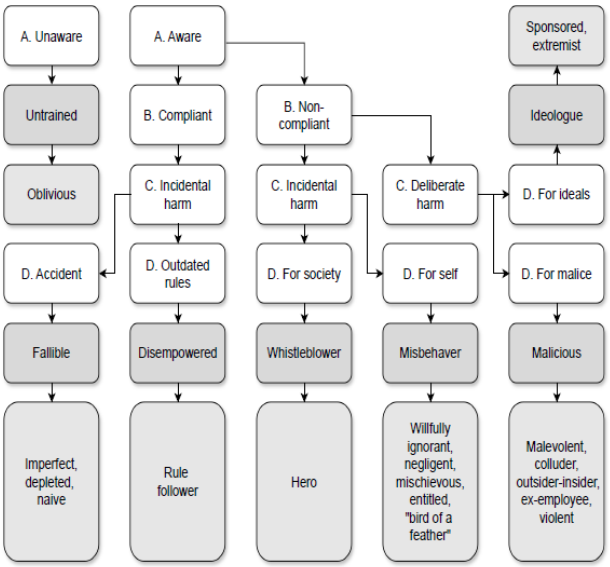

Figure 2. An Example Taxonomy from the Literature (adopted from [37])

The insider threat taxonomies may be useful for organizations in terms of risk analysis. When knowing an organization's valuable assets, it is possible to better analyze typical and plausible insider threats.

As assets vary from an organization to another, so do the insider threats. For instance, it has been suspected that some intentional data leaks from central governments have involved insiders with political goals [39]. Such insiders would be classified into ideologues. The assets of most multinational companies are entirely different than politically relevant documents, and thus also the insider threats are typically quite different. In terms of empirical research, however, it remains unclear how useful the taxonomies are in practice. The insider types might be useful in criminology research, for instance, but the problem is that there are no easily and publicly available datasets for caught insiders from organizations themselves, law enforcement, or other public authorities. Yet, in terms of theoretical research, taxonomies are analytically useful already because intentions and goals connote with motives. Together, intentions, goals, and motives (or desires) constitute a formidable conundrum in philosophy and

moral psychology [40]. However, it is unnecessary to delve deeper into this problem area already because the insider threat literature sampled is not theoretically rich in this regard. It is typically assumed that malicious insiders are more or less rational in their actions.

4.2. Theoretical Foundations

Motives of malicious insiders constitute a central theoretical tenet in literature. In particular, the so-called situational crime prevention (SCP) theory posits that a crime occurs because of two factors: a motive and an opportunity [41]. Then, a crime can often be prevented simply by removing either factor from the equation. In terms of insider threats and cybersecurity, a motive might be countered by rigorous logging, monitoring, and auditing, which help to hold culprits accountable, while opportunities might be reduced by fine-grained authentication and authorization procedures, strict access controls, and other related defensive cybersecurity measures [42, 43].

Figure 3. The Fraud Diamond

Together, such technical solutions should increase the risk of getting caught, the effort required for an insider to commit an offense, and the probability of obtaining a reward from the offense. In terms of reducing the probability of obtaining rewards, many additional techniques can be implemented; among these are digital signatures and watermarking, information and hardware segregation, encryption, automatic data destruction schemes, and minimization of reconnaissance information [44]. While these techniques may not fully prevent an insider incident from happening, they should still discourage employees or other associated people from misconduct.

These preventive techniques make the SCP a close associate of another criminological theory, the so-called general deterrence theory. According to this theory, criminals make decisions based on the perceived utility (or benefits) of their actions and the costs (or sanctions) involved. Increasing the costs is achieved by deterrence, meaning that an organization should at least invest in education and outreach to inform employees or other relevant people about the penalties from misconduct [41]. Deterrence is essentially about external factors, like many other organizational measures, such as monetary rewards from a job well done, but psychologically also intrinsic factors are relevant [45]. Traditionally, intrinsic motivation refers to an inherent desire to undertake work even without specific rewards, but the concept can be also extended toward the insider threat context. For instance, an employee's intrinsic motivation to comply with an organization's security policies may be weakened by poor job satisfaction, among other things.

Furthermore, to some extent, the SCP aligns with a rational choice viewpoint to crime according to which crimes are deliberate; a motive to commit a crime correlates with an intention of obtaining some reward, whether financial resources or material goods, prestige, excitement, or something else [46, 47]. This viewpoint is implicitly present also in the popular so-called fraud diamond or triangle (see Fig. 3) that contains three angles corresponding with a motive (or a pressure), an opportunity, and rationalization [48–51]. The rationalization refers to the rational means by which criminals justify their actions to themselves.

Oftentimes, such a justification involves contemplating a reward. For instance, an indebted insider might rationally justify his or her offense due to the fact that he or she needs to pay his or her bills. Rationalization may also apply to non-malicious insiders. For instance, a person might share a password with a colleague because he or she rationalizes that no one cares about such a supposedly minor violation of an organization's security policy. To counter such rationalization and associated excuses, organizations should seek to have clear documents on policies and their enforcement [43, 44, 48, 52]. These also include guidelines on ethical conduct, intellectual property, and trade secrets, among other things. There is also existing research on such policies implemented in large information technology companies [53]. Despite the name of the rational choice viewpoint, it is usually assumed that criminals still operate only in terms of so-called bounded or limited rationality; they do not have perfect information available in the environment in which criminal decision-making takes place [47]. To this end, some authors have considered thresholds for decision-making involving an intention to commit a crime based on judgments from limited information cues [8, 46, 54, 55]. In addition to a lack of information, psychological and related factors presumably further reduce rationality and rational decision-making.

The theory of reasoned action (TRA) is a popular general theory for explaining human behavior [56]. It posits that behavioral intentions, which motive actual behavior, are composed of two factors: attitudes and subjective norms. The former are shaped by the expected outcomes of a given behavior, while subjective norms include the perceived social pressure to perform or not to perform a given action. These tenets correlate with the earlier points about the other theories; expected outcomes may refer to the rewards from an offense, for instance, while social pressure and other subjective norms may include knowledge about deterrence measures. The insider threat literature has considered also an extension to the TRA, the so-called theory of planned behavior (TPB). It augments the TRA with perceived behavioral control, meaning the difficulty or ease of performing a given

behavioral action [34]. Again, the TPB's behavioral control can be interpreted in the insider threat context to align with the opportunities in the SCP. The analytical meaning of the TBP (and TRA) is illustrated in Fig. 4.

The social pressure in the TRA and the behavioral control in the TPB further pinpoint toward two other theories, the so-called social bond theory (SBT) and the social learning theory. The SBT posits that strong social bonds may prevent an offender from committing a crime, despite the offender's inclination to commit the crime. In reverse: bonding with criminals or other misbehavers may increase the probability that an insider will commit an offense. Such bonding is the message from the social learning theory; a person is more likely to commit a crime if he or she associates with those who do so or those who transmit delinquent ideas [41, 57]. Therefore, both theories can be seen to fall into a domain of a more general sociological social identity theory; a person tends to behave in ways that comply with the norms of formal and informal groups to which the person belongs [58]. The actual social bonds in the SBT are broken down into four types: attachment (such as an affection and respect toward an organization), commitment (such as an effort and energy to support the organization's goals), involvement (such as a participation in organizational activities), and beliefs (such as values and views about the organization) [44].

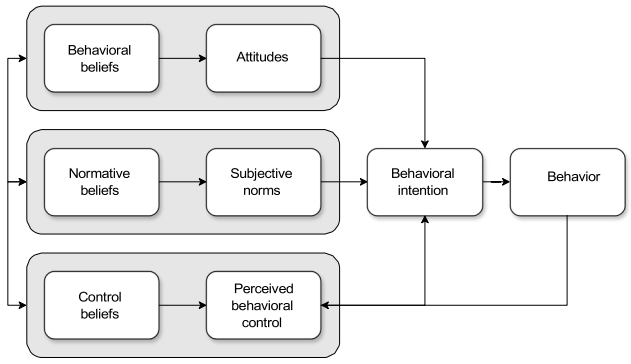

Figure 4. The TPB in Essence (adopted from [34])

Strengthening such bonds should then reduce the probability of insider incidents in an organization. The actual measures may range from improving workplace culture to increasing the efficiency of human resource management and seeking responsible leadership. Such measures and the resulting bonds are closely related to the trust-related theorizing in the literature [54, 59, 60]. Despite technical and organizational security measures, management should ideally trust its employees and the other way around; on one hand, a high-trust organizational environment is likely to decrease the probability of insider incidents. On the other hand, abuses of trust by people in positions of trust are a typical reason behind insider incidents. This trust conundrum is not necessarily easy to address because trust takes a long time to develop, and restrictive security controls may decrease trust among staff. This point is implicitly behind a further theory, the so-called social exchange theory (SET) according to which employees reciprocate their employer's treatment of them [61]. Thus: if an employee is mistreated, he or she is likely to misbehave.

Finally, there is a general and rather straightforward ecological theory in sociology, criminology, and associated social sciences: a person's past behavior is likely to affect his or her future behavior [58]. Among other things, this theory justifies much recruitment practices; past educational and employment history together with formative experiences are central to most hiring decisions. In criminology and criminal law, the theory is implicitly also behind a long-lasting debate on reductionism in criminal justice systems; there are no easy answers to a question whether general crime prevention and intervention should be based on past criminal behavior and associated profiling [62]. With this point in mind, the personal characteristics of insiders can be considered alongside the personal situations in which insiders find themselves.

4.3. Personal Characteristics and Personal Situations

The aforementioned theories supplement presumptions about the personal characteristics of an insider offender and his or her personal situation. Both can be seen as more or less objective facts, not psychological assumptions about a person, although both are likely to also influence the person's psychological state and the other way around. In line with the ecological theory, formal background checks done by law enforcement or intelligence agencies almost always involve checking a person's criminal record [58]. Clearly, then, having an existing (cyber) crime record can be seen to increase the probability that a person will commit an offense [51]. Another example: having a Ph.D. in cybersecurity is also an objective fact about a person's characteristics. Such a qualification may then correlate with the opportunity in the SCP and maybe the motive too; the person in question may have (inside or outside) knowledge of how to evade an organization's technical security controls and hide his or her tracks.

Indeed, the literature reviewed tends to agree that technical knowledge, skills, and competencies are relevant factors for insider threats [11, 52, 60, 63–66]. In fact, many documented insider incidents have involved employees in technical professions, such as system administrators, database operators, or programmers [60]. Technical competency tends to also reduce the effectiveness of deterrence measures [67]. To these ends, some authors have augmented the SCP to include also the capability of an insider to perform an attack [4], while others have considered skills in conjunction with the opportunities [48]. There are also other theoretical and practical loose ends with respect to competencies and capabilities. For instance, technical knowledge and skills may correlate with a person's psychological traits, such as curiosity and aspiration for exploration, which, in turn, may constitute a

motive for a cyber-crime [16]. Another point is that highly qualified people may be more familiar with an organization's security policy. To use the Ph.D. example again: a person with such a qualification is likely also better aligned toward ethical guidelines and professional conduct. Of course, such a presumption is dependent on context. For instance, when compared to a blue-collar worker, a scientist may be more prone to steal intellectual property to start a business [68]. This example would connote with a motive to conduct a misconduct as well as the personal characteristics.

Regarding even more fundamental personal characteristics, the literature is surprisingly silent about basic demographic factors. Only in passing are such factors rarely mentioned in the literature. For instance, it has been mentioned that male employees in senior positions are more likely to commit offenses [51], although also the contrary has been partially observed; older employees are less likely to become malicious insiders [16, 36]. In addition to gender and seniority, ethno-cultural factors have been mentioned [8]. These factors have also been mentioned with respect to susceptibility to phishing and social engineering attacks [69], which, as said, are also relevant for insider threats. These uncommon remarks notwithstanding, a rigorous and systematic evaluation of demographic factors is absent from the literature surveyed.

A further point is that the literature has often considered only technical capabilities and competencies, omitting social and other "softer" skills. According to SBT, such skills are likely to increase bonding with an organization, which should reduce the probability of misconduct. To this end, job engagement and bonding with coworkers have been considered [61]. There are also studies that have examined symbolic interactions in groups and their relation to the trust worthiness of the persons involved [70]. In addition, social isolation and remote work have been considered as risk factors [52]. These studies align, either explicitly or implicitly, with SBT's basic theoretical premises. In addition, there are studies that are perhaps closer to the SET than the SBT. For instance, some studies have considered organizational culture, ethics, and organizations' support for employees to do their work as pull-off factors for insider threats [8]. Here, particularly the organizational support is a good example of the reciprocity assumption behind the SET. Furthermore, there are studies that align, again either explicitly or implicitly, with the TPB and its behavioral attitudes. A good example would be job satisfaction and its relation to insider threats [71, 72]. Also other attitudes, ideologies, subjective norms, and values have been considered, such as patriotism, civil disobedience, disloyalty, and dislike of authorities [11, 41, 52, 69].

Figure 5. The MICE Acronym

However, literature offers no cues on how the bonding, reciprocity, attitudes, and related factors are related to a person's characteristics, such as his or her people skills. Furthermore, personal characteristics, like personality traits, are mostly static, whereas the factors mentioned are rather dynamic. Therefore, also the motives are often not static but instead develop or change over time [8, 60]. For instance, a person's job satisfaction may increase over time, which should imply that the probability of he or she becoming a malicious insider decreases over time. Likewise, bonding with coworkers takes time. A further example would relate to the SET. If a person is continuously mistreated, the probability may progressively increase that he or she will eventually commit a misconduct.

The dynamic nature of the factors mentioned correlate with a personal situation of an insider; an employee continuously finds himself or herself in new situations during his or her career and life in general. Here, the literature has been particularly keen to examine different "trigger factors" that prompt an insider to attack an organization from inside. A term precipitating events has also been used to describe such triggers [65]. Such events or trigger factors justify the term pressure in the fraud diamond; there is often not only a motive but a specific pressure for a person to commit a misconduct. Although not part of the literature reviewed, the so-called MICE acronym is illuminating in this context (see Fig. 5). It is a mnemonic identifying some major factors that make a person prone to recruitment of foreign intelligence services: money, ideology, compromise, and ego [73]. As already said, ideology and politics may motive and trigger some insiders, but according to the literature, money is a more typical factor. The financial situation of a person is also an objective fact.

Indeed, the typical pressures considered in the insider threat literature are financial problems and vices that a person have, a person's family situation, termination of his or her employment contract, and negative organizational changes [11, 51, 57, 64, 68, 74]. According to the literature, many insider incidents have occurred soon after a person has left an organization either through a resignation or a layoff; therefore, both contract termination dates and contract expiration dates have been used as proxy variables for predicting insider threats [4, 68]. Also, the type of a contract (full-time or part-time) has been considered [64]. These variables likely correlate with a financial pressure a

person may have. In other words, a heavily indebted employee with a part-time contract termination in sight may be a good candidate for becoming a malicious insider. The negative organizational changes may include a high staff turnover [4], wage reductions [57, 68], or an assignment of persons to new but undesired work roles, among other things. In addition, the literature has considered negative evaluations, corrective actions, and warnings as predictors [57, 60, 64, 75]. Although only seldom contemplated, these factors and the associated pressures or triggers may also change a person's psychological state. Before considering such states, further or less static elements of human beings should be elaborated.

4.4. Personality Traits

Many of the papers sampled have considered different personality traits as relevant factors for predicting insider threats or considering risks thereto. A personality trait is a relatively stable habitual pattern of behavior, thought, and emotion. Depending on a theory and operationalization, a personality trait can be dichotomous, meaning that a person either has or has not a given trait, or these can be seen to operate in an interval or continuous scale, such as when the end-points correspond with extraversion and introversion. Table 1 shows a summary of the traits considered in the literature sampled.

The summary does not mean that a given paper would necessarily operate with a given trait empirically; many papers have also considered traits as theoretical building blocks or illustrative examples on psychological factors in the insider threat context. Nor does the summary include all traits considered in literature. As soon discussed, some were omitted due to theoretical and other problems in literature. As could be expected, much of the literature has operated with the so-called "big five" personality traits. These traits, which were initiated already in the late 1950s but which gained prominence in the early 1990s [88], are the de facto ones used in contemporary empirical literature, regardless of discipline. Also, the so-called "dark triad", as pioneered in the early 2000s [89], has been quite frequently used or discussed in the literature reviewed. This triad is composed of three offensive but non-pathological personality types: machiavellianism, narcissism, and psychopathy. Of these and other "dark traits", it has been suspected that particularly non-pathological psychopathy might be a good predictor for insider threats, although many of the darker personality traits can be seen also as strong predictors of performance in cybersecurity jobs [36, 66]. Non-pathological machiavellianism and psychopathy are reportedly also decent predictors for determining engagement in fraudulent behavior more generally [49]. Literature has also considered traits that align directly with the MICE acronym discussed earlier. In other words, a big ego and a markedly self-centered personality have been perceived as risk factors for insider threats [16, 41, 75]. In addition, literature has operated with numerous other personality traits, some of which are problematic or even questionable, as soon elaborated.

There are many problems in the literature empirically dealing with the personality traits or otherwise justifications on why these or other traits should correlate with insider threats [57, 77, 80, 81, 83, 86]. There are three probable reasons for this atheoretical tenet in literature. The

Table 1. Examples of Personality Traits Considered in Literature

Trait	Papers
The "big five" traits:	
Conscientiousness	[11, 55, 57, 71, 72, 74, 76–86]
Agreeableness	[11, 55, 57, 71, 72, 74, 76–83, 85, 86]
Neuroticism	[11, 55, 57, 71, 72, 74, 76–83, 85, 86]
Openness	[11, 57, 72, 74, 76–78, 80–83, 85, 86]
Extraversion	[11, 57, 72, 74, 76–78, 80–83, 85, 86]
The "dark triad" traits:	
Narcissism	[2, 11, 36, 49, 66, 74, 77, 80, 85]
Machiavellianism	[11, 36, 49, 66, 74, 77, 80, 85]
Psychopathy	[11, 36, 49, 66, 74, 77, 80, 85]
Other dark traits:	
Hostility	[11, 36, 57]
Manipulativeness	[36, 75]
Deceitfulness	[36]
Anti-sociality	[11]
Sadism	[11]
Other traits or sub-dimensions:	
Impulsiveness	[2, 11, 36, 87]
Honesty and humility	[11, 36, 84]
Self-assurance	[57, 85]
Dutifulness	[36, 85]
Fearfulness	[11, 57]
Empathy	[7, 11]
Entitlement	[11, 77]
Excitement seeking	[11, 71]
Self-centeredness	[41, 75]
Excitableness	[36]
Skepticism	[36]
Callousness	[75]
Cautiousness	[36]
Reservedness	[36]
Leisureness	[36]
Boldness	[36]
Mischievousness	[36]
Colorfulness	[36]
Imaginativeness	[36]

Trait	Papers
Diligentness	[36]
Sympathy	[85]
Resilience	[11]
Joviality	[57]
Attentiveness	[57]
Shyness	[57]

first reason is partly historical and partly related to the availability of data: the big five traits have long been a part of the popular insider threat datasets released by the CERT Coordination Center at Carnegie-Mellon university. The second reason is disciplinary: because most of the papers are in the domain of computer science, rich psychological theorizing is not expected, unlike machine learning and related applications.

The third reason is computational: particularly the big five traits are easily available through scientific libraries or ready-made online frameworks, such as the IBM's Watson artificial intelligence platform.

The computational aspects lead to a further problem: it is difficult to deduce about the validity of the traits used in the literature because some papers have used surveys [57, 77, 84], sometimes with validated psychometric scales [36, 49], and even professional personality testing services [82], while others have relied on text mining methods. In terms of the latter, particularly email datasets and occasionally social networking data have been used together with sentiment analysis [78–80, 85]. The methodological uncertainties gain more weight in case personality traits are used in real-world situations. Besides privacy issues, legal obstacles, and organizational ethics, poorly conducted personality tests, likely including those done via machine learning, perhaps without awareness of the employees involved, may put people into unfavorable or unpleasant situations. Organizational trust may be involved too, among other things; a person wrongly assigned as having psychopathic traits, for instance, may no longer trust the given organization. Alternatively: either current or prospective employees are not likely to answer candidly to questions involving particularly the dark triad traits [66]. This point reiterates the inherent methodological problems.

In terms of academic research and the literature reviewed, there are three additional methodological and theoretical problems worth noting. The first problem is that some studies have included only some of the big five traits. As these are typically not statistically independent, multicollinearity may provide a justification, but a theoretical rationale for omitting some traits is typically lacking [71, 79]. Some papers speak about a "difficult personality factor", as composed of neuroticism, conscientiousness, and agreeableness, based on previous studies that have indicated that the traits mentioned correlate with anti-social behavior [55]. While anti-social behavior is in line with the SBT's social bonding assumptions, it remains unclear why openness and extraversion would not be relevant for predicting insider threats. Indeed, on one hand, some studies have included excitement-seeking, which is a facet of extraversion, as a predictor for insider threats [11, 71]. As noted in the previous section, curiosity and exploration, which likely correlate with excitement-seeking, are often considered as relevant when investigating motives for cyber-crimes. On the other hand, some papers have found that openness, extraversion, and agreeableness are relevant predictors, but with a reverse interpretation; people who are creative, social, and helpful to others are less likely to commit insider offenses [76]. These conflicting interpretations underline the literature's problems in theorizing.

The second problem is closely related: already the big five traits contain numerous sub-dimensions of personality. Hence, it is unclear whether some "traits" considered in the literature really are personality traits. The examples include trust, fear, guilt, anger, sadness, sympathy or empathy, morality, altruism, and dutifulness [11, 57, 79, 85]. Of these, at least empathy and trust in others belong to the agreeableness trait [71], and amorality either to the machiavellianism or psychopathy trait [49]. The same goes with factors such as concealment of things from others [55], which might be a sub-dimension of openness. Furthermore, some of the "traits" mentioned, such as fear, guilt, sadness, and anger, are clearly emotions, not stable personality traits of a person. The situation becomes even more complex once the collusion between insiders and external threats is considered; already many of the big five traits correlate with personal vulnerabilities to social engineering attacks [33, 38, 82]. Thus, as has been argued also in the literature reviewed [36], due to the inherent complexity, including statistical problems, "less might be more" when operating with personality traits.

The third problem follows: some studies have included "traits" that are psychological disorders rather than conventional personality traits. The examples include depression, borderline personality disorder, paranoia, and disruptive mood dysregulation disorder [11, 63]. To put aside the question whether these might be considered traits of a person's personality, validity remains a big issue with such factors. As correctly noted in the literature, these and related disorders or "traits" would require a clinical diagnosis [71]. The literature has also discussed questionable "disorders" present in popular discourse, such as FOMO (fear of missing out) and problematic Internet use [2]. Like previously with "traits" that are not necessarily traits, it remains unclear whether these "disorders" really are disorders. Furthermore, it also remains unclear how useful, or plausible such factors are in practical settings, including an organization's human resource management, risk analysis procedures, and potential insider threat predictions.

Thus, all in all, it is difficult to make systematic theoretical sense of literature operating with personality traits. It suffices to conclude that personality traits do correlate with a likelihood of insider offenses, but the theoretical reasons remain undecipherable. There is also the more fundamental debate in psychology over the validity of the big five and other traits to begin with. In addition to widespread measurement issues, personality

traits typically also vary across other factors, such as age, gender, and cultural settings [36]. The critical points raised align with other critical view-points expressed in the literature surveyed. None of the personality traits are inherently good or bad, and many of these also correlate with job performance, security awareness, and so-called cyber hygiene practices [84, 90]. Therefore, instead of engaging in intrusive psychological profiling with problematic methodologies and potentially dangerous false positives, it might be a good idea for organizations to use psychology for better motivating employees, including with respect to cybersecurity practices [60]. This final point aligns well with the general theoretical premises in the SBT and SET.

4.5. Psychological States

The literature reviewed has thus far addressed theoretical foundations, personal characteristics, personal situations, and personality traits. Of these, personal characteristics are relatively stable and rather objective facts about a person, such his or her educational qualifications, expertise and employment history, or a criminal record. Also, personality traits are rather stable and long-term habitual patterns; a person may be bold and extrovert, and such fundamental personality traits are unlikely to change substantially and rapidly through the person's life. In contrast, personal situations are dynamic and may change quite rapidly. While financial problems may pile up over the years, it is also possible that a person with a gambling habit loses a large amount of money in one night. When compared to personal characteristics and personality traits, the dismissal of a person from a job is also a more dynamic sequence; he or she may receive prior warnings, but the firing event may still come as a surprise. It is also possible that a whole company will suddenly go bankrupt, and all its employees are dismissed without prior warnings. These examples again illustrate the pressures, triggers, and precipitating events discussed earlier. In what follows, particularly these pressures, triggers, and events are discussed in relation to a person's "psychological state". Before continuing further, three additional brief remarks are in order. The first is about the literature reviewed: there are some papers that have considered "psychological profiles", "psychological features", or some analogous constructs, but without proving any details on what such profiles or features contain and on which theoretical and methodological premises they rely on [91–93]. Clearly, it is impossible to engage with such papers any further. The second point is about terminology: the concept of a psychological state is not well-established in psychology. While there seems to be no rigorous definitions, the literature reviewed has understood psychological states to correspond with a person's psychological make-up and his or her emotional state, both of which may change as a result of an environment [65]. The make-up includes personality traits as well as diagnosed disorders, such as, say, clinical depression. It should be acknowledged that a given behavioral pattern may express different psychological states at different times, and different persons may share the same psychological state [94]. In other words, two depressed people may have different personality traits and other personal characteristics, and the same behavioral pattern that led to a person's diagnosis may not lead to a further diagnosis. In any case, as psychological make-ups were already addressed to the extent possible with the literature reviewed, emotions are what is left to tackle. The third point follows: again, there are no rigorous definitions, but emotion can be generally understood as a physical and mental state associated with thoughts, feelings, and behavioral responses. It is worth picking an insight from the phenomenology of emotions; these are almost always directed toward something [95]. While some emotions may be self-directed, others are directed toward other people or objects. A further point is about the dynamics of emotions; these may develop and manifest themselves over a long period of time, such as perhaps with a love of one's special other, or these may manifest themselves as sudden outbursts, such as might be the case with, say, outrage over something or some object. In the insider threat context, the direction toward which emotions are targeted may be a given organization itself or the human beings working in the organization, such as coworkers or executives. Emotions may be directed also toward clients, customers, stakeholders, or other related parties of an organization.

With these preliminary points in mind, Table 2 shows a summary of typical emotions considered in literature. As previously with the personality traits, the summary is neither fully complete nor does it imply that a given paper would operate with a given emotion empirically or otherwise discuss it in detail. It is also worth remarking that similar conceptual and theoretical issues are present than with personality traits. For instance, revenge has been listed as an emotion [16], although it is a behavioral pattern involving commitment of a harmful action in response to real or perceived grievances. In any case, revenge has been seen as a frequent motive for insider attacks; in some papers it even surpasses a motive for financial gains or a motive around opportunities [11]. Revenge is usually also an emotionally laden hostile action taken by a person.

Table 2. Examples of Emotions Considered in Literature

Emotion	Papers
Stress	[4, 16, 33, 35–37, 41, 50, 55, 57, 61, 65, 74,
Disgruntlement	[7, 8, 16, 37, 41, 55, 57, 61, 65, 74, 75]
Anger	[16, 37, 41, 55, 57, 63, 65, 75, 85]
Frustration	[16, 65]
Anxiety	[33, 85]
Fear	[65]

Emotion	Papers
Boredom	[65]
Jealousy	[74]
Shame	[97]
Guilt	[97]

Among the frequently discussed emotions is disgruntlement toward an organizations or people working in it. It might be due to a denied promotion, a lack of recognition, a mistreatment, or some other organizational reason [37, 75]. Therefore, organizations should generally seek to avoid unnecessary provocations in sensitive workplace matters, as these may arouse disgruntlement and other strong negative emotions [43]. Then, literature usually assumes that disgruntlement in particular motives a revenge toward an organization, which, in turn, eventually leads to an attack from inside the organization. Though, some papers assume that disgruntlement first leads to counterproductive behavior before an actual attack takes place [55]. Such counterproductive behavior might include browsing job search portals or sending complaints to supervisors and coworkers via electronic mail [98], or it may include generally confrontational behavior [41], among other things. Nevertheless, disgruntlement remains the primary emotional trigger in this line of thought and research.

Anger and stress are further commonly discussed emotions in literature. To put aside the question whether and how much anger and disgruntlement are related, both are good examples for six reasons. First, stress, a feeling of emotional strain and pressure, does not come out from the blue sky but develops over time. Therefore, it correlates with other factors, such as work performance [33, 35], which, in turn, may correlate with job evaluations and a person's attitudes toward an organization. A similar point applies also to other emotions. For instance, a disgruntled employee may under-perform in his or her work, which may cause poor job evaluations or even lead to disciplinary action, which, in turn, may cause the employee to become even more disgruntled [65].

Another example would relate to exploration; as an insider engages in a transgression, his or her curiosity increases, which may make it more difficult for him or her to stop his or her misbehavior [9]. Although presumably difficult to empirically observe, such vicious cycles are likely a risk factor for insider threats. In general, however, literature has not considered the intensification of particular emotions beyond the examples mentioned.

The second point follows: nor has literature considered the fact that particular emotions may lead to further, different emotions. To use stress again as an example: a heavily stressed employee may ask supervisors to reduce his or her workload, but if his or her request is declined, the employee may become angry toward the supervisors or the organization in general. If the situation lasts for a long period of time, stress and anger may then lead to disgruntlement, which may lead to ideas about revenge, which may motive an insider attack. This kind of a vicious cycle resembles the reciprocity assumption in the SET. Of course, it may also be that stress alone is a trigger factor for an insider attack.

The third point is closely related: the emotions expressed by other people are likely to affect a person's own emotions. While stress as an emotion is supposedly mostly self-directed, an employee may become angry or even disgruntled if he or she also observes that coworkers express cheerfulness and joy at work, perhaps due to lighter workloads, real or perceived. To some extent, this point has been considered in the literature; an employee's disposition is affected by the dispositions of other employees [8]. Therefore, it is no wonder that coworkers who have witnessed an (unintentional) insider incident have shown feelings of guilt, embarrassment, and frustration [96]. Broadly speaking, these points are underneath the bonding assumptions in SBT. The social learning theory provides a further point: if a stressed employee only bonds with other stressed employees, they may all eventually become jointly angry or express other negative emotions.

The fourth point is related to the previous discussion: not only may emotions arouse from other people or an environment, including a given organization, but a person's own situation is also a source of emotions. Here, as could be expected, the literature has pointed out that financial pressures and other problems in a person's life increase the stress levels of the person [57, 61]. A similar point applies to other emotions. For instance, a person may become angry at himself or herself or at other people due to problems in his or her own life. Closer to insider threats, a dismissal of an employee is likely to arouse negative feelings.

Fifth, low stress tolerance and poor anger management have been seen as risk factors for insider threats [11, 41]. The ability to handle stress, anger, and other emotions is partially a learned ability and partially related to a person's personality. Thus, stress levels have been observed to correlate with personality traits, such as agreeableness, conscientiousness, and narcissism [85]. This point further complicates the predictions done with personality traits; some traits may predict insider threats, but it may also be that some traits, possibly even the same traits, improve a person's stress tolerance and anger management, which should reduce the probability of insider attacks either directly or due to the emotions relation to disgruntlement. It may even be that personality traits should be used as confounding factors toward emotions, which may be the actual source for insider threat risks. Furthermore, some personality traits, such as the dark ones, tend to better or only manifest themselves in high-stress situations [36]. Some traits may also correlate with a tendency to feel guilt or shame, which may prevent an insider from conducting a transgression even in case he or she has already planned one [97]. Together, these points add further weight to the critical reflection presented in the previous section.

The sixth and last point is about the technical approaches for insider threat detection: intrusive monitoring and

profiling are likely to cause stress among employees [50]. Also, other negative side-effects may be present, including alienation of employees, reduction in morale, and decreasing creativity [61]. This final point serves to highlight that the technical approaches to insider threats are not without their own problems; in some cases, they may even be counterproductive.

Finally, it should be mentioned that in addition to surveys and other conventional research methods, sentiment analysis has again been prominent in literature for profiling emotions. Emails [99–103], visited web pages [99–101], and social media [104] have provided the typical sources for empirical data. These approaches repeat the previous point: it remains unclear how such intrusive profiling fits into the legal landscape, workplace culture, and organizational ethics, and how potential employees might perceive the profiling and what consequences their perceptions might have. Furthermore, there is also the important question of how well sentiments correspond with actual emotions.

4.6. Games, Deception, and Neurology

Literature contains also three branches of research that do not connect well with the other papers and the themes presented in them, although all branches are still to some extent related to psychology. Already due the SLR protocol used, these branches need a brief elaboration.

The first branch is about different games. Unlike what might be expected, these are not typically game-theoretic games but rather concrete games involving different tests and cognitive puzzles performed under stressful conditions [77]. There are also studies investigating games for detecting lying [80], simulating betrayals [105], and detecting deceptive behavior from textual cues [106]. Also, behavioral data from mainstream online games has been investigated [78]. The second branch is closely related: there are some studies that have investigated the use of deception and honeypots for detecting insider threats [77, 107, 108]. Although the connection to psychology remains implicit in both branches, the themes discussed and investigated still presumably correlate with psychological make-ups, including personality traits and emotions.

The last branch is about biometrics and neurology. In terms of the former, eye tracking has been a popular choice for insider threat detection [109]. It has also been used together with neurological approaches. For instance, eye tracking has been used in conjunction with functional magnetic resonance imaging (fMRI) in order to test the reception of security messages under emotional constraints [110]. Alternatively, eye tracking has also been used in conjunction with electroencephalogram (EEG) signals for detecting insider threats [111]. As has been correctly observed in the literature, such neurological data is highly sensitive personal data, which may thus be a subject for insider threats in itself [112]. Also, other security and privacy risks have been acknowledged in the literature [113, 114]. Furthermore, it remains unclear how useful, ethical, and legal these approaches are in practice. If psychological profiling is seen as intrusive, clearly brain scanning is even more intrusive. Thus, it remains debatable whether current or prospective employees would consent to fMRI or EEG scanning, and whether labor and privacy laws would even allow such scanning at a workplace.

5. Conclusion

What do we know about the psychology of insider threats? At first glance, the answer might be: not much. On a second thought, the literature reviewed posits a general picture in which personal characteristics, personal situations, and other more or less objective facts correlate with personality traits, psychological states, and different behavioral patterns. However, (a) One of the most prominent gaps in the research is the lack of comprehensive and well-developed theoretical frameworks that connect personal traits, psychological states, and behavior to insider threat behavior. Although literature frequently references psychological theories, especially those borrowed from sociology, criminology, and related fields, these references are often only implicit. The lack of a unified theory that explicitly connects psychological concepts to insider threat behavior leaves many causal relationships undefined and under-theorized. Without a clear theoretical foundation, it becomes challenging to predict or explain why certain psychological traits or conditions might lead to insider threat behavior in particular contexts.

Another research gap follows: (b) there is a general lack of validation and replication studies as well as pre-registered studies. Although some attempts have been made [10], this lack together with the absence of comparable theories, implies that meta-analysis is generally impossible. In other words, (c) it remains impossible to say which theories outperform other theories. Even more importantly, (d) it is also impossible to say whether the technical approaches outperform the non-technical approaches, including those based on psychology. As was discussed in Sections 4.4, 4.5, and 4.6, psychological and related profiling is generally problematic in terms of privacy, ethics, workplace culture, and even law. Even though psychology remains an important topic in academic insider threat research, it would therefore be important to know whether the technical approaches suffice alone for insider threat detection; that is, whether psychological profiling is even needed in practical settings. In terms of academic research, furthermore, with some rare exceptions [76], (e) the literature reviewed has mostly operated with static snapshots of data. As was pointed out in Sections 4.3 and 4.5, neither motives nor emotions are static; therefore, more longitudinal research is generally needed in order to better understand insider threats and their psychology. Finally, (f) there are some methodological and related problems in the literature. Among other things, proxy variables have been quite loosely and liberally used for probing different psychological aspects of persons. This

criticism also affects machine learning approaches. For instance, it remains debatable how well sentiment analysis can proxy actual emotions of persons.

As has been pointed out also in other reviews [10], also other conventional issues may be present, including so-called publication bias. Among other things, (g) negative results, including nonworking or implausible methodological approaches are also missing from literature. For instance, there is a noticeable absence of negative or inconclusive results—studies that fail to find patterns or that demonstrate that certain methods or theories do not work. This lack of negative results distorts the overall picture and may overstate the effectiveness of certain approaches. The omission of negative findings limits our understanding and impedes scientific progress by not providing a full view of what works and what does not. Finally, and importantly, (h) the SLR protocol used indicated no relevant papers published in psychology journals. This suggests that psychology, while often referenced in insider threat research, has not been fully integrated into the core academic literature on the topic. The lack of psychology-based research in reputable psychology journals means that the field of insider threats may not be benefiting from the latest advances in psychological theory and methodology.

Hence, the gaps in the current research on the psychology of insider threats present a critical need for more comprehensive, interdisciplinary frameworks. The lack of clear theoretical connections between psychological factors and insider behavior limits our ability to predict and prevent these threats effectively. The absence of replication studies, longitudinal research, and negative findings distorts our understanding of what truly works in both technical and psychological approaches. By addressing these gaps, the field can advance toward more reliable, scientifically grounded methods for detecting and mitigating insider threats. Only by integrating psychological insights more thoroughly into insider threat research can we develop solutions that are both effective and ethically sound.

References

[1] Ruohonen, J. and Saddiqa, M. (2025) What Do We Know About the Psychology of Insider Threats. In Forthcoming (in press) in the Proceedings of the 15th EAI International Conference on Digital Forensics & Cyber Crime (EAI ICDF2C 2024), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (Volume 613) (Dubrovnik: Springer).

[2] Mathews, R. (2017) Interrogating "Privacy" in a World Brimming with High Political Entanglements, Surveillance, Interdependence & Interconnections. Health and Technology 7: 265–324.

[3] Ruohonen, J., Hjerppe, K. and von Zastrow, M. (2024) An Exploratory Case Study on Data Breach Journalism. In Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024) (Vienna: ACM): 1–9.

[4] Elmrabit, N., Yang, S., Yang, L. and Zhou, H. (2020) Insider Threat Risk Prediction Based on Bayesian Network. Computers & Security 96: 101908.

[5] CISA (2023) Zero Trust Maturity Model. Cybersecurity & Infrastructure Security Agency (CISA) of the United States. Available online in July 2024: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

[6] Santos, E., Nguyen, H., Yu, F., Kim, K.J., Li, D., Wilkinson, J.T., Olson, A. et al. (2012) Intelligence Analyses and the Insider Threat. IEEE Transactions on Systems, Man, and Cybernetic – Part A: Systems and Humans 42(2): 331–347.

[7] Sarkar, K.R. (2010) Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures. Information Security Technical Report 15: 112–133.

[8] Sokolowski, J.A., Banks, C.M. and Dover, T.J. (2016) An Agent-Based Approach to Modeling Insider Threat. Computational and Mathemtical Organization Theory 22: 273–287.

[9] Zaytsev, A., Malyuk, A. and Miloslavskaya, N. (2017) Critical Analysis in the Research Area of Insider Threats. In Proceedings of the IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud) (Prague: IEEE): 288–296.

[10] Gheyas, I.A. and Abdallah, A.E. (21016) Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis. Big Data Analytics 1(6): 1–29.

[11] Marbut, A.R. and Harms, P.D. (2024) Fiends and Fools: A Narrative Review and Neo-Socioanalytic Perspective on Personality and Insider Threats. Journal of Business and Psychology 39: 679–696.

[12] Akello, B.O. (2024) Organizational information security threats: Status and challenges. World Journal of Advanced Engineering Technology and Sciences 11(1): 148–162.

[13] Alzaabi, F.R. and Mehmood, A. (2024) A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access 12: 30907–30927.

[14] Al-Shehari, T.A., Rosaci, D., Al-Razgan, M., Alfakih, T., Kadrie, M., Afzal, H. and Nawaz, R. (2024) Enhancing insider threat detection in imbalanced cybersecurity settings using the density-based local outlier factor algorithm. IEEE Access 12: 34820–34834.

[15] Lavanya, P. and Shankar Sriram, V. (2022) Detection of insider threats using deep learning: A review. Computational Intelligence in Data Mining: Proceedings of ICCIDM 2021 : 41–57.

[16] Prabhu, S. and Thompson, N. (2022) A Primer on Insider Threats in Cybersecurity. Information Security Journal: A Global Perspective 31(5): 602–611.

[17] Alcover, C.M., Rico, R., Turnley, W.H. and Bolino, M.C. (2017) Understanding the changing nature of psychological contracts in 21st century organizations: A multiple-foci exchange relationships approach and proposed framework. Organizational Psychology Review 7(1): 4–35.

[18] Gioe, D.V. and Hatfield, J.M. (2021) A damage assessment framework for insider threats to national security information: Edward snowden and the cambridge five in comparative historical perspective. Cambridge Review of International Affairs 34(5): 704–738.

[19] Anderson, P.D. (2022) On moderate and radical government whistleblowing: Edward snowden and julian assange as theorists of whistleblowing ethics. Journal of media ethics 37(1): 38–52.

[20] Schoenherr, J.R., Lilja-Lolax, K. and Gioe, D. (2022) Multiple approach paths to insider threat (map-it): Intentional, ambivalent and unintentional insider threats. Counter-Insider Threat Research and Practice 1(1).
[21] Jones, L.A. et al. (2024) Unveiling human factors: Aligning facets of cybersecurity leadership, insider threats, and arsonist attributes to reduce cyber risk. SocioEconomic Challenges 8(2): 44–63.
[22] Goel, S., Williams, K. and Zavoyskiy, S. (2016) Stopping insiders before they attack: Understanding motivations and drivers .
[23] Shah, S.I., Shahjehan, A. and Afsar, B. (2022) Leading machiavellians on the road to better organizational behavior. Personnel Review 51(5): 1604–1626.
[24] Freeman, D., Garety, P.A., Kuipers, E., Fowler, D. and Bebbington, P.E. (2002) A cognitive model of persecutory delusions. British Journal of Clinical Psychology 41(4): 331–347.
[25] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.K.R. and Burnap, P. (2020) Impact and key challenges of insider threats on organizations and critical businesses. Electronics 9(9): 1460.
[26] Dugo, T. (2007) The insider Threat to Organizational Information Security: A Structural Model and Empirical Test. Ph.D. thesis.
[27] Jurrens, R.D. (2013) Fool me once: Us v. aleynikov and the theft of trade secrets clarification act of 2012. Berkeley Tech. LJ 28: 833.
[28] Rice, C. and Searle, R.H. (2022) The enabling role of internal organizational communication in insider threat activity–evidence from a high security organization. Management Communication Quarterly 36(3): 467–495.
[29] Nightingale, A. (2009) A Guide to Systematic Literature Reviews. Surgery 27(9): 381–384.
[30] Kitchenham, B. and Brereton, P. (2013) A Systematic Review of Systematic Review Process Research in Software Engineering. Information and Software Technology 55: 2049–2075.
[31] Hiebl, M.R.W. (2023) Sample Selection in Systematic Literature Reviews of Management Research. Organizational Research Methods 26(2): 229–261.
[32] Petersen, K., Feldt, R., Mujtaba, S. and Mattson, M. (2008) Systematic Mapping Studies in Software Engi- neering. In Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineer- ing (EASE) (Italy: BCS Learning & Development Ltd.): 68–77.
[33] Greitzer, F.L., Strozer, J.R., Cohen, S., Moore, A.P., Mundie, D. and Cowley, J. (2014) Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In Proceedings of the IEEE Security and Privacy Workshops (IEEE): 236–250.
[34] Lahcen, R.A.M., Caulkins, B., Mohapatra, R. and Kumar, M. (2020) Review and Insight on the Behavioral Aspects of Cybersecurity. Cybersecurity 3: 1–18.
[35] Carroll, T.E., Greitzer, F.L. and Roberts, A.D. (2014) Security Informatics Research Challenges for Mitigating Cyber Friendly Fire. Security Informatics 13: 1–14.
[36] Harms, P., Marbut, A., Johnston, A.C., Lester, P. and Fezzey, T. (2022) Exposing the Darkness Within: A Review of Dark Personality Traits, Models, and Measures and Their Relationship to Insider Threats. Journal of Information Security and Applications 71: 103378.
[37] Renaud, K., Warkentin, M., Pogrebna, G. and van der Schyff, K. (2024) VISTA: An Inclusive Insider Threat Taxonomy, With Mitigation Strategies. Information & Management 61: 103877.
[38] Uebelacker, S. and Quiel, S. (2014) The Social Engineering Personality Framework. In Proceedings of the Workshop on Socio-Technical Aspects in Security and Trust (Vienna: IEEE): 24–30.
[39] Ruohonen, J., Hjerppe, K. and Kortesuo, K. (2024) Crisis Communication in the Face of Data Breaches. Archived manuscript. Available online in June: https://arxiv.org/abs/2406.01744.
[40] Chan, D.K. (2008) Introduction: Moral Psychology Today. In Chan, D.K. [ed.] Moral Psychology Today: Essays on Values, Rational Choice, and the Will (Cham: Springer).
[41] Azaria, A., Richardson, A., Kraus, S. and Subrahmanian, V.S. (2014) Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data. IEEE Transactions on Computational Social Systems 1(2): 135–155.
[42] Køien, G.M. (2019) Why Cryptosystems Fail Revisited. Wireless Personal Communication 106: 85–117.
[43] Safa, N.S., Maple, C., Furnell, S., Azad, M.A., Perera, C., Dabbagh, M. and Sookhak, M. (2019) Deterrence and Prevention-Based Model to Mitigate Information Security Insider Threats in Organisations. Future Generation Computer Systems 97: 587–597.
[44] Safa, N.S., Maple, C., Watson, T. and Von Solms, R. (2018) Motivation and Opportunity Based Model to Reduce Information Security Insider Threats in Organisations. Journal of Information Security and Applications 40: 247–257.
[45] Lee, D., Lallie, H.S. and Michaelides, N. (2023) The Impact of an Employee's Psychological Contract Breach on Compliance with Information Security Policies: Intrinsic and Extrinsic Motivation. Cognition, Technology & Work 25: 273–289.
[46] Sokolowski, J.A. and Banks, C.M. (2015) An Agent Based Approach to Modeling Insider Threat. In Proceedings of the Symposium on Agent-Directed Simulation (San Diego: ACM): 36–41.
[47] Willison, R. and Backhouse, J. (2006) Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective. European Journal of Information Systems 15: 403–414.
[48] Farahmand, F. and Spafford, E.H. (2013) Understanding Insiders: An Analysis of Risk-Taking Behavior. Information Systems Frontiers 15: 5–15.
[49] Harrison, A., Summers, J. and Mennecke, B. (2018) The Effects of the Dark Triad on Unethical Behavior. Journal of Business Ethics 153: 53–77.
[50] Mekonnen, S., Padayachee, K. and Meshesha, M. (2015) A Privacy Preserving Context-Aware Insider Threat Prediction and Prevention Model Predicated on the Components of the Fraud Diamond. In Proceedings of the Annual Global Online Conference on Information and Computer Technology (GOCICT) (Louisville: IEEE): 60–65.
[51] Othman, R. and Ameer, R. (2022) In Employees We Trust: Employee Fraud in Small Businesses. Journal of Management Control 33: 189–213.
[52] Kisenasamy, K., Perumal, S., Raman, V. and Singh, B.S.M. (2022) Influencing Factors Identification in Smart Society for Insider Threat in Law Enforcement Agency Using a Mixed Method Approach. International Journal of System Assurance Engineering and Management 13(Suppl 1): 236–251.
[53] Dong, B., Chernov, S. and Akpina, K.O. (2024) Legal Aspects of Corporate Systems for Preventing Cybercrime

Among Personnel. Crime, Law and Social Change 81: 75–96.
[54] Martinez-Moyano, I.J., Rich, E.H., Conrad, S.H. and Andersen, D.F. (2006) Modeling the Emergence of Insider Threat Vulnerabilities. In Proceedings of the Winter Simulation Conference (Monterey: IEEE): 562– 568.
[55] Sticha, P.J. and Axelrad, E.T. (2016) Using Dynamic Models to Support Inferences of Insider Threat Risk. Computational and Mathemtical Organization Theory 22: 350–381.
[56] Fishbein, M. and Ajzen, I. (1977) Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Philosophy and Rhetoric 10(2): 130–132.
[57] Dupuis, M. and Khadeer, S. (2016) Curiosity Killed the Organization: A Psychological Comparison Between Malicious and Non-Malicious Insiders and the Insider Threat. In Proceedings of the 5th Annual Conference on Research in Information Technology (Boston: ACM): 35–40.
[58] Binns, C.A. and Kempf, R.J. (2021) Background Checks: The Theories Behind the Process. Security Journal 34: 776–801.
[59] Gill, M. and Crane, S. (2017) The Role and Importance of Trust: A Study of the Conditions that Generate and Undermine Sensitive Information Sharing. Security Journal 30: 734–748.
[60] Munshi, A., Dell, P. and Armstrong, H. (2021) Insider Threat Behavior Factors: A Comparison of Theory With Reported Incidents. In Proceedings of the 45th Hawaii International Conference on System Sciences (Maui: IEEE): 2402–2411.
[61] Moore, A.P., Cassidy, T.M., Theis, M.C., Bauer, D., Rousseau, D.M. and Moore, S.B. (2018) Balancing Organizational Incentives to Counter Insider Threat. In Proceedings of the IEEE Security and Privacy Workshops (SPW) (IEEE): 237–246.
[62] Prins, S.J. and Reich, A. (2018) Can We Avoid Reductionism in Risk Reduction? Theoretical Criminology 22(2): 258–278.
[63] Ahmad, M.B., Saeed-ur-Rehman, Akram, A. and Asif, M. (2014) Towards a Realistic Risk Assessment Methodology for Insider Threats of Information Misuse. In Proceedings of the 12th International Conference on Frontiers of Information Technology (Islamabad: IEEE): 176–181.
[64] Faresi, A.A. and Wijesekera, D. (2011) Preemptive Mechanism to Prevent Health Data Privacy Leakage. In Proceedings of the International Conference on Management of Emergent Digital EcoSystems (San Francisco: ACM): 17–24.
[65] Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R.T. and Whitty, M. (2014) Understanding Insider Threat: A Framework for Characterising Attacks. In Proceedings of the IEEE Security and Privacy Workshops (San Jose: IEEE): 214– 228.
[66] Sanders, G.L., Upadhyaya, S. and Wang, X. (2019) Inside the Insider. IEEE Engineering Management Review 47(2): 84–91.
[67] D'Arcy, J. and Hovav, A. (2009) Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. Journal of Business Ethics 89: 59–71.
[68] Al tabash, K. and Happa, J. (2018) Insider-Threat Detection Using Gaussian Mixture Models and Sensitivity Profiles. Computers & Security 77: 838–859.
[69] Dalal, R.S., Howard, D.J. and Brummel, B.J. (2022) Organizational Science and Cybersecurity: Abundant Opportunities for Research at the Interface. Journal of Business and Psychology 37: 1–29.
[70] Ho, S.M. and Benbasat, I. (2014) Dyadic Attribution Model: A Mechanism to Assess Trustworthiness in Virtual Organizations. Journal of the Association for Information Science and Technology 65(8): 1555–1576.
[71] Axelrad, E.T., Sticha, P.J., Brdiczka, O. and Shen, J. (2023) A Bayesian Network Model for Predicting Insider Threats. In Proceedings of the IEEE Security and Privacy Workshops (San Francisco: IEEE): 82–89.
[72] Sepehrzadeh, H. (2023) A Method for Insider Threat Assessment by Modeling the Internal Employee Interactions. International Journal of Information Security 22: 1385–1393.
[73] Petkus, D.D. (2010) Ethics of Human Intelligence Operations: Of MICE and Men. International Journal of Intelligence Ethics 1(1): 97–121.
[74] Whitelaw, F., Riley, J. and Elmrabit, N. (2024) A Review of the Insider Threat, a Practitioner Perspective Within the U.K. Financial Services. IEEE Access 12: 34752–34768.
[75] Greitzer, F.L. and Purl, J. (2022) The Dynamic Nature of Insider Threat Indicators. SN Computer Science 3: 1– 15.
[76] Alhajjar, E. and Bradley, T. (2022) Survival Analysis for Insider Threat. Computational and Mathematical Organization Theory 28: 335–351.
[77] Basu, S., Chua, Y.H.V., Lee, M.W., Lim, W.G., Maszczyk, T., Guo, Z. and Dauwels, J. (2018) Towards a Data-Driven Behavioral Approach to Prediction of Insider-Threat. In Proceedings of the IEEE International Conference on Big Data (Big Data) (Seattle: IEEE): 4994– 5001.
[78] Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E. et al. (2012) Proactive Insider Threat Detection Through Graph Learning and Psychological Context. In Proceedings of the IEEE Symposium on Security and Privacy Workshops (San Francisco: IEEE): 142–149.
[79] Brown, C.R., Watkins, A. and Greitzer, F.L. (2013) Predicting Insider Threat Risks Through Linguistic Analysis of Electronic Communication. In Proceedings of the 46th Hawaii International Conference on System Sciences (Wailea: IEEE): 1849–1858.
[80] Chi, H., Scarllet, C., Prodanoff, Z.G. and Hubbard, D. (2016) Determining Predisposition to Insider Threat Activities by Using Text Analysis. In Proceedings of the Future Technologies Conference (FTC) (San Francisco: IEEE): 985–990.
[81] Duan, S., Yuan, J. and Wang, B. (2024) Contextual Feature Representation for Image-Based Insider Threat Classification. Computers & Security 140: 103779.
[82] Eftimie, S., Cotenescu, V., Răcuciu, C. and Glăvan, D. (2021) A Case Study in Anticipating Insider Vulnerabilities Using Psychological Profiling. In Proceedings of the IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) (Bucharest: IEEE): 1–4.
[83] Ren, X. and Wang, L. (2020) A Hybrid Intelligent System for Insider Threat Detection Using Iterative Attention. In Proceedings of 2020 6th International Conference on Computing and Data Engineering (ACM): 189–194.
[84] Schoenherr, J.R. (2022) Insider Threats and Individual Differences: Intention and Unintentional Motivations. IEEE Transactions on Technology and Society 3(3): 175– 184.
[85] Yang, G., Cai, L., Yu, A., Ma, J., Meng, D. and Wu, Y. (2018) Potential Malicious Insiders Detection Based on a Comprehensive Security Psychological Model. In Proceedings of the IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService) (Bamberg): 9–16.

[86] Yousef, R., Jazzar, M., Eleyan, A. and Bejaoui, T. (2023) A Machine Learning Framework & Development for Insider Cyber-Crime Threats Detection. In Proceedings of the International Conference on Smart Applications, Communications and Networking (Smart-Nets) (Istanbul: IEEE): 1–6.
[87] Roy, K.C. and Chen, G. (2024) GraphCH: A Deep Framework for Assessing Cyber-Human Aspects in Insider Threat Detection. IEEE Transactions on Dependable and Secure Computing (Preprint): 1–15.
[88] Goldberg, L.R. (1993) The Structure of Phenotypic Personality Traits. American Psychologist 48(1): 26–34.
[89] Paulhouse, D.L. and Williams, K.M. (2002) The Dark Triad of Personality: Narcissism, Machiavellianism, and Psychopathy. Journal of Research in Personality 36(6): 556–563.
[90] Schoenherr, J.R. and Thomson, R. (2021) The Cybersecurity (CSEC) Questionnaire: Individual Differences in Unintentional Insider Threat Behaviours. In Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (Dublin: IEEE): 1–8.
[91] Bishop, M., Gates, C., Frincke, D. and Greitzer, F.L. (2009) AZALIA: An A to Z Assessment of the Likelihood of Insider Attack. In Proceedings of the IEEE Conference on Technologies for Homeland Security (Waltham: IEEE): 385–392.
[92] Gamachchi, A. and Boztaş, S. (2015) Web Access Patterns Reveal Insiders Behavior. In Proceedings of the International Workshop on Signal Design and its Applications in Communications (IWSDA) (Bengaluru: IEEE): 70–74.
[93] Li, C., Li, F., Yu, M., Guo, Y., Wen, Y. and Li, Z. (2022) Insider Threat Detection Using Generative Adversarial Graph Attention Networks. In Proceedings of the IEEE Global Communications Conference (GLOBECOM) (Rio de Janeiro: IEEE): 2680–2685.
[94] Block, N.J. and Fodor, J.A. (1972) What Psychological States Are Not. The Philosophical Review 81(2): 159–181.
[95] Szanto, T. and Landweer, H. (2020) Introduction: The Phenomenology of Emotions—Above and Beyond 'What It Is Like to Feel'. In Szanto, T. and Landweer, H. [eds.] The Routledge Handbook of Phenomenology of Emotion (Oxford: Routledge), 1–37.
[96] Khan, N., Houghton, R.J. and Sharples, S. (2022) Understanding Factors That Influence Unintentional Insider Threat: A Framework to Counteract Unintentional Risks. Cognition, Technology & Work 24: 393–421.
[97] Farshadkhah, S., Van Slyke, C. and Fuller, B. (2021) Onlooker Effect and Affective Responses in Information Security Violation Mitigation. Computers & Security 100: 102082.
[98] Kan, X., Fan, Y., Zheng, J., Kudreyko, A., Chi, C., Song, W. and Tregubova, A. (2023) User-Level Malicious Behavior Analysis Model Based on the NMF-GMM Algorithm and Ensemble Strategy. Nonlinear Dynamics 111: 21391–21408.
[99] Jiang, J., Chen, J., Choo, K.R., Liu, K., Liu, C., Yu, M. and Mohapatra, P. (2018) Prediction and Detection of Malicious Insiders' Motivation Based on Sentiment Profile on Webpages and Emails. In Proceedings of the IEEE Military Communications Conference (MILCOM) (Los Angeles: IEEE): 1–6.
[100] Jiang, J., Chen, J., Gu, T., Choo, K.R., Liu, C., Yu, M., Huang, W. et al. (2019) Warder: Online Insider Threat Detection System Using Multi-Feature Modeling and Graph-Based Correlation. In Proceedings of the IEEE Military Communications Conference (MILCOM) (Norfolk: IEEE): 1–6.
[101] Legg, P.A., Buckley, O., Goldsmith, M. and Creese, S. (2017) Automated Insider Threat Detection System Using User and Role-Based Profile Assessment. IEEE Systems Journal 11(2): 503–512.
[102] Mittal, A. and Garg, U. (2023) Prediction and Detection of Insider Threat Detection Using Emails: A Comparision. In Proceedings of the Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) (Trichirappalli): 1–6.
[103] Soh, C., Yu, S., Narayanan, A., Duraisamy, S. and Chen, L. (2019) Employee Profiling via Aspect-Based Sentiment and Network for Isider Threats Detection. Expert Systems With Applications 135: 351–361.
[104] Osterritter, L. and Carley, K.M. (2021) Conversations Around Organizational Risk and Insider Threat. In Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ACM): 613–621.
[105] Ho, S.M. and Warkentin, M. (2017) Leader's Dilemma Game: An Experimental Design for Cyber Insider Threat Research. Information Systems Frontiers 19: 377–396.
[106] Ho, S.M., Hancock, J.T., Booth, C., Burmester, M., Liu, X. and Timmarajus, S.S. (2016) Demystifying Insider Threat: Language-Action Cues in Group Dynamics. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS) (Koloa: IEEE): 2729–2738.
[107] Alohaly, M., Balogun, O. and Takabi, D. (2022) Integrating Cyber Deception Into Attribute-Based Access Control (ABAC) for Insider Threat Detection. IEEE Access 10: 108965–108978.
[108] Takabi, H. and Jafarian, J.H. (2017) Insider Threat Mitigation Using Moving Target Defense and Deception. In Proceedings of the 2017 International Workshop on Managing Insider Security Threats (ACM): 93–96.
[109] Yerdon, V.A., Lin, J., Wohleber, R.W., Matthews, G., Reinerman-Jones, L. and Hancock, P.A. (2022) Eye-Tracking Active Indicators of Insider Threats: Detecting Illicit Activity During Normal Workflow. IEEE Transactions on Engineering Management 69(6): 3838–3847.
[110] Anderson, B.B., Vance, A., Kirwan, C.B., Eargle, D. and Jenkins, J.L. (2016) How Users Perceive and Respond to Security Messages: a NeuroIS Research Agenda and Empirical Study. European Journal of Information Systems 25: 364–390.
[111] Hashem, Y., Takabi, H., Dantu, R. and Nielsen, R. (2017) A Multi-Modal Neuro-Physiological Study of Malicious Insider Threats. In Proceedings of the 2017 International Workshop on Managing Insider Security Threats (Dallas: ACM): 33–44.
[112] Ienca, M., Haselager, P. and Emanuel, E.J. (2018) Brain Leaks and Consumer Neurotechnology. Nature Biotechnology 36(9): 805–810.
[113] Choi, S. and Zage, D. (2012) Addressing Insider Threat Using "Where You Are" as Fourth Factor Authentication. In Proceedings IEEE International Carnahan Conference on Security Technology (ICCST) (Newton: IEEE): 147–153.
[114] Kritika, M. (2024) A Comprehensive Study on Navigating Neuroethics in Cyberspace. AI and Ethics (Published online in May): 1–8.