NCITE NATIONAL COUNTERTERRORISM, INNOVATION, TECHNOLOGY, AND EDUCATION CENTER
A U.S. DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Examining Best Practices in Threat Assessment from an Insider Threat Perspective

A Review and Integration: Interim Deliverable

Matt Allen, Kat Parsons, Tin Nguyen, and Lauren Zimmerman
National Counterterrorism Innovation, Technology, and Education Center

About NCITE. The National Counterterrorism Innovation, Technology, and Education (NCITE) Center was established in 2020 as the Department of Homeland Security (DHS) Center of Excellence for counterterrorism and terrorism prevention research. Sponsored by the DHS Science and Technology Directorate Office of University Programs, NCITE is the trusted DHS academic consortium of over 60 researchers across 18 universities and non-government organizations. Headquartered at the University of Nebraska at Omaha, NCITE is a leading U.S. academic partner for counterterrorism research, technology, and workforce development.

Acknowledgement. The research in this report was conducted in support of Award no. 70RSAT219R00000021, “Public Safety and Violence Prevention Evaluation,” from the Department of Homeland Security (DHS) Science and Technology Directorate under Basic Ordering Agreement 70RSAT21G00000002.

Disclaimer. Any opinions or conclusions contained herein are those of the authors and do not necessarily reflect those of the Department of Homeland Security, the DHS Science and Technology Directorate, or the University of Nebraska System.

TABLE OF CONTENTS

INTRODUCTION

The purpose of this report is to examine behavioral threat assessment from an insider threat perspective through an extant literature review. Broadly defined, *insider threats* generally refer to individuals, such as employees, contractors, or former employees, with privileged access to organizational information, locations, or systems who have the potential to cause harm. These threats can be intentional (malicious) or unintentional (non-malicious), with intentional threats being of most interest to the current purpose. These intentional threats can be further categorized into specific threat incidents or outcomes, such as sabotage, theft of intellectual property, fraud, espionage, and targeted violence.[1] This contrasts with *behavioral threat assessment* (often referred to simply as "threat assessment," used for the remainder of the report), which is typically concerned with understanding potential threats of violence in different settings (Meloy et al., 2021).

Both definitions consider the threat that an *individual actor* (rather than a group) poses, but the definition of "insider threat" is broader in the sense of the *outcomes and targets* considered. Specifically, definitions of insider threat consider threats to individuals, systems, and to the larger organization. "Threat assessment," while largely concerned with physical harm to individuals, is broader in the sense of *context*, which includes additional locations such as public places and schools in addition to the workplace. Threat assessment also includes special consideration of targets, such as intimate partners and public figures. These similarities and differences are illustrated in Figure 1.

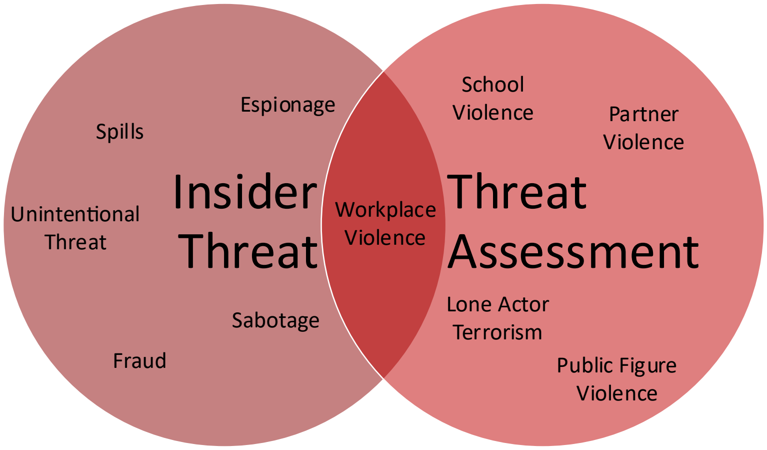


Figure 1. Venn Diagram of Threat Assessment and Insider Threat Practice Areas

There are several reasons to examine threat assessment from an insider threat perspective:

1. **The extant insider threat literature draws on different disciplines than what is typically found in the threat assessment literatures**. As illustrated in Figure 2, insider threat has

[1] See, for example, the National Insider Threat Task Force [NITTF] mission fact sheet, insider threat training provided by the Center for Development of Security Excellence [CDSE], and the Cybersecurity & Infrastructure Security Agency's [CISA] insider threats page.

emerged as an area of concern more recently compared to threat assessment, driven by (a) high profile espionage insider threat cases in the U.S. federal government (e.g., Robert Hanssen[2]), (b) the emergence of computer technology as an opportunity for malicious insiders to cause significant harm with relative ease (Pfleeger & Caputo, 2012), and (c) the increasing costs of insider threat incidents to organizations (e.g., IBM Security, 2020; Ponemon Institute, 2022).

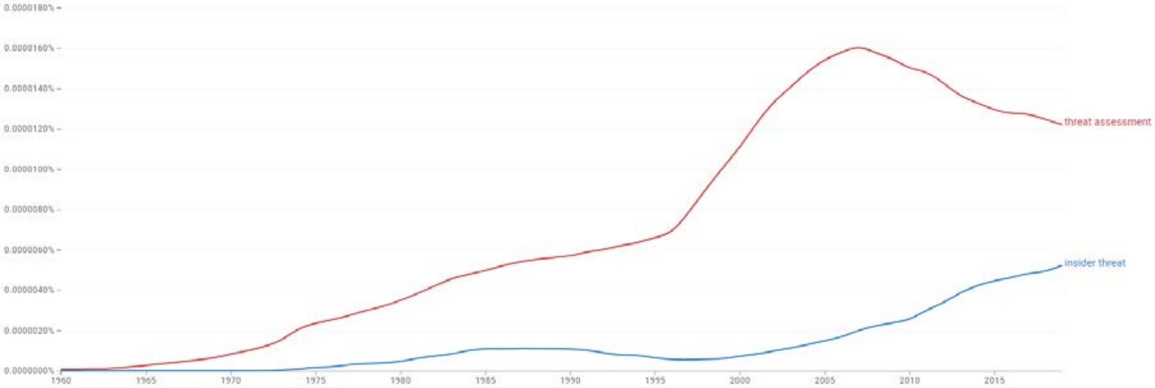


Figure 2. Frequency of terms “Insider Threat” and “Threat Assessment”[3]

Specifically, there is a substantial information security/cybersecurity literature examining types, antecedents, and interventions of insider threat incidents (see Homoliak et al., 2019 for a review), and using these examinations to develop testable models for predicting and preventing such incidents (see Bedford & van der Laan, 2021; Greitzer et al., 2019; Lenzenweger & Shaw, 2022; and Witty, 2021, for examples). Thus, there are models and empirical data available in the insider threat literature that may inform the practice of threat assessment.

2. **Insider threats are studied in an organizational context**. The organizational context has several benefits. First, as alluded to in the previous point, there are data available in organizational contexts that are not readily available in other settings, such as schools and public places. For example, organizations routinely collect data on individual differences (e.g., through pre-employment assessments, trainings), behavior on the job (e.g., through performance reviews, citations for rule violations, absences), and behavior on organizational networks (e.g., attempts to gain unauthorized access, activity logs). Consequently, models of insider threat and associated interventions tend to be more specified and have more empirical support than their threat assessment counterparts. While there is not one-to-one correspondence between insider threat and physical

[2] https://www.fbi.gov/history/famous-cases/robert-hanssen

[3] “The Google Ngram Viewer displays user-selected words or phrases (ngrams) in a graph that shows how those phrases have occurred in a corpus. Google Ngram Viewer's corpus is made up of the scanned books available in Google Books.” Source: https://infoguides.gmu.edu/textanalysistools/ngram#:~:text=About%20Google%20Ngram%20Viewer,books%20available%20in%20Google%20Books.

violence in other settings, a deeper understanding of the insider threat perspective allows us to examine promising avenues for understanding threat assessment more generally.

A second benefit of the organizational context is the ability to leverage organizational sciences, such as economics, industrial/organizational psychology, and management, to further inform counter-insider threat theory and practice (Dalal et al., 2022). Insider threat researchers and practitioners have begun to recognize the limitations of an exclusively *command-and-control* approach (i.e., focused on compliance and external controls) in countering insider threats, and the potential impact positive incentives in reducing the probability of threat incidents (Baweja et al., 2022; Moore et al., 2016; 2022). Organizational scientists have studied these *positive deterrence* (i.e., those that increase employee job satisfaction, well-being, performance) factors for decades and are thus well-suited to inform current practice.

3. **Threat assessment practitioners recognize the role of insider threats**. According to recent interviews with 13 threat assessment professionals (NCITE, 2022a), insider threats are relevant to the work done by threat assessment teams in at least three ways. First, insider threat teams tracking network behavior can refer employees exhibiting virtual behaviors of concern to threat assessment teams for follow up. Second, threat assessment teams can refer employees exhibiting behaviors of concern for additional monitoring, particularly in cases where the individual of concern has the opportunity and capability to retaliate to a perceived grievance via cyberattack. Third, threat assessment teams are frequently working with insiders, and thus should be aware of any special considerations or data sources that can be leveraged in their assessment.

In summary, much can be gained by examining threat assessment from an insider threat perspective and by incorporating related literature areas. To realize these gains, the report contains the following sections:

Part 1: Insider Threat Literature Review. In this section, we begin with a brief overview of the counter insider threat research and models of insider threat. This helps to situate the remainder of the report in the larger context of this literature. In particular, it contextualizes our emphasis in the remainder of the report on three types of malicious insider threats of particular interest to public sector entities – espionage, sabotage, and workplace violence – as they are most relevant to the threat assessment context. We conclude this section with a discussion of limitations of the insider threat literature when applying to threat assessment practice.

Part 2: Literatures Related to Insider Threat. We build off Part 1 by supplementing the counter-insider threat research with relevant (a) security and (b) social and behavioral science literatures. The social and behavioral sciences section applies lessons learned from a range of disciplines, including criminology, psychology, and management, to the question of how malicious insiders can be better detected and deterred.

Conclusion and Next Steps. The current report summarizes the literatures that we are drawing upon to develop new insights related to insider threat. In this section, we will summarize key conclusions at a high level and describe next steps underway on this effort.

PART 1: INSIDER THREAT LITERATURE REVIEW

Our first step in this research was to obtain a broad-based understanding of extant insider threat literature. Specifically, our goal was to obtain peer-reviewed research articles to answer the following two questions:

1. How is insider threat understood and operationalized?
2. What predictive models exist for insider threat, and how are those structured?

To accomplish this, we searched several research databases[4] using the following Boolean phrase as a search starting point: ("insider threat*" OR "insider risk") AND ("model*" OR "framework*" OR "typolog*" OR "paradigm" OR "category*" OR "taxonom*" OR "ontology" OR "predict*" OR "mediat*" OR "moderat*" OR "critical pathway*"). After the initial search, restrictions were excluded from the search of social and behavioral science databases (e.g., PsycINFO) as the initial search yielded very few or no articles.

We supplemented this search with known research-backed industry resources for answering these questions, such as the technical reports found on the websites for Defense Personnel and Security Research Center (PERSEREC)[5] and Carnegie Mellon University's Software Engineering Institute (SEI, specifically the CERT Division)[6]. As expected, the vast majority of articles came from information security/cybersecurity or similarly situated resources. Given this finding, the remainder of this section summarizing definitions and models of insider threat heavily emphasizes that literature.

Defining Insider Threats

Due to shifts in the workplace, such as from physical to digital storage and from manual to knowledge work, the study of insider threat is prevalent in the information systems and technologies (IS&T) field, to include IT and cybersecurity. Indeed, the term "insider threat" gained prominence in industry due to data breaches from malicious insiders (Capelli et al., 2012). There are several definitions of insider threat in the IS&T literature, which vary on (a) definitions of an "insider", (b) consideration of maliciousness, and (c) treatment of access. See Appendix A for some example definitions and Homoliak and colleagues (2019) for a review.

Defining an "Insider"

Definitions of insider threat vary regarding who qualifies as an insider (see Appendix A for example definitions). Because information technology is digital (and therefore easily sharable), it is possible when collaborating to easily share documents or provide access to those outside the company. Some definitions are concerned only with those who are employees, while others see anyone who was given access to a system (e.g., a contractor) as an insider. For example, Butts

[4] IEEE Xplore, ACM Digital Library, PsychInfo, ABI/INFORM Global, Criminal Justice Abstracts, ProQuest Academic Complete; others searched yielded no results
[5] https://www.dhra.mil/PERSEREC/Selected-Reports/
[6] https://www.sei.cmu.edu/publications/technical-papers/index.cfm

and colleagues (2005) define an insider as "… any individual who has been granted any level of trust in an information system" (p. 413). Others provide more specificity, ranging from, "a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure" (Bishop et al., 2008; p. 5) to more technical definitions, such as, "an individual who has the knowledge of the organization's information system structure to which he/she has authorized access and who knows the underlying network topologies of the organization's information systems" (p. 240; Althebyan & Panda, 2007).

Maliciousness

One way to categorize insiders is by intent—malicious vs. negligent (Bailey et al., 2018; Carlson, 2020). Malicious insiders are those who, "intentionally used … access… that negatively affected … the organization's information or information systems" (Costa et al., 2016; p. 1). While negligent insiders are typically considered unintentional (i.e., non-malicious), some insiders, such as those accessing unauthorized information to satisfy a curiosity, can be both negligent and malicious if the accessed information is then part of a threat event. Bailey et al. (2018) illustrate this situation in their analysis of the Vocabulary for Event Recording and Incident Sharing (VERIS) database, where 44 percent of the insider-related breaches were rooted in negligence or co-opting of organizational resources. They demonstrate how a negligent insider may not intend to cause harm to the company but may instead use their access for their own self-interests, such as accessing client records to get contact information to ask an individual out on a date. Another way to understand intent is through the end goal of the action. For Band et al. (2006), they see actions against the IT systems as either insider sabotage or espionage—is the insider hoping to harm the organization for their own interests (sabotage) or are they working on behalf of another party (espionage)? Some scholars further distinguish these incidents more by separating IT sabotage, theft of intellectual property, and fraud (Capelli et al., 2012). Others disagree with using insider threat as an umbrella under which sabotage and espionage fall under, instead separate espionage, sabotage, and insider threat into their own categories, while acknowledging that there may be overlap (Bulling et al., 2008).

Access

A second way to categorize insiders is the route taken to access a system. Alawneh and Abbadi (2011) understand this as whether the access credentials were obtained through authorized or unauthorized means, and whether the access to a system was legitimate. The *authorization* of credentials is whether the organization gave the insider the credentials or not, whereas the *legitimate* access is whether the insider was supposed to use their credentials to access that system or not. Another way of thinking about this is that some researchers focus on whether the insider stole the key to access a room or if it was given to them by the organization (Alawneh & Abbadi, 2011), while others are interested in if the insider was supposed to use their key to open that door or not, or even be in the room at all (Bishop and Gates, 2008; Elmrabit et al., 2015). An extension of this category is the type of insider and their authorization level.

Summary

As described above, definitions of insider threat tend to vary in terms of (a) “insider” definition, (b) maliciousness, and (c) access. In general, older definitions of insider threat contain more specificity while more recent definitions tend to be more inclusive. For example, SEI CERT’s definition of an insider shifted from, “A current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data,” to "an individual who has or had authorized access to an organization’s assets" in recent years (Zimmer et al., 2022; p. 2:3). Similarly, older definitions of insider threat focus more on violations of IT security policies (e.g., Bishop, 2005; Bishop & Gates, 2008; Theoharidou et al., 2005;). However, a consistent element across definitions is the insider misusing their privileges, to potentially include unintentional acts (Elmrabit et al, 2020; Greitzer et al., 2016).

Based on the above, we can conclude the following:

1. **Defining “insider threat” is complex.** Several elements impact how insider threat is defined. Recent definitions have generally become more inclusive to incorporate the full range of potential individuals and expressions of insider threat.
2. **There are several ways to define insiders and insider threat.** That said, we agree with the more general definitions, such as that provided by the National Insider Threat Task Force (NITTF) (see Appendix A). However, while this general definition covers the full threat landscape, our analysis for the remainder of the paper will focus on malicious (as opposed to negligent/non-malicious) insiders with privileged access to government (as opposed to private sector) resources.

With a working definition of insider threat in hand, we turn our attention to IS&T-oriented models to predict insider threats and threat events.

Models of Insider Threat

A foundational model for determining insider threat risk is referred to as the “critical pathway” model. Shaw and Sellers (2015), in their description of the model, posited, based on empirical insider threat research, “that there exists a common set of factors and a similar pattern of individual and organizational behavior across the many occurrences during recent years” (p. 1). This model suggests that factors, including personal predispositions, personal and professional stressors, concerning behaviors, and problematic organizational responses increase the probability of a hostile act. The last factor (problematic organizational responses) is particularly critical in this model, as adaptive or maladaptive responses by the organization can increase or reduce the probability of a threat event. Another notable feature of the model is that it considers the complexity of human behavior in making judgments, making it a good foundation for Structure Professional Judgment (SPJ) tools (Lenzenweger & Shaw, 2022). This model has proved foundational in the scholarship and practice around insider threat and is illustrated in Figure 3.

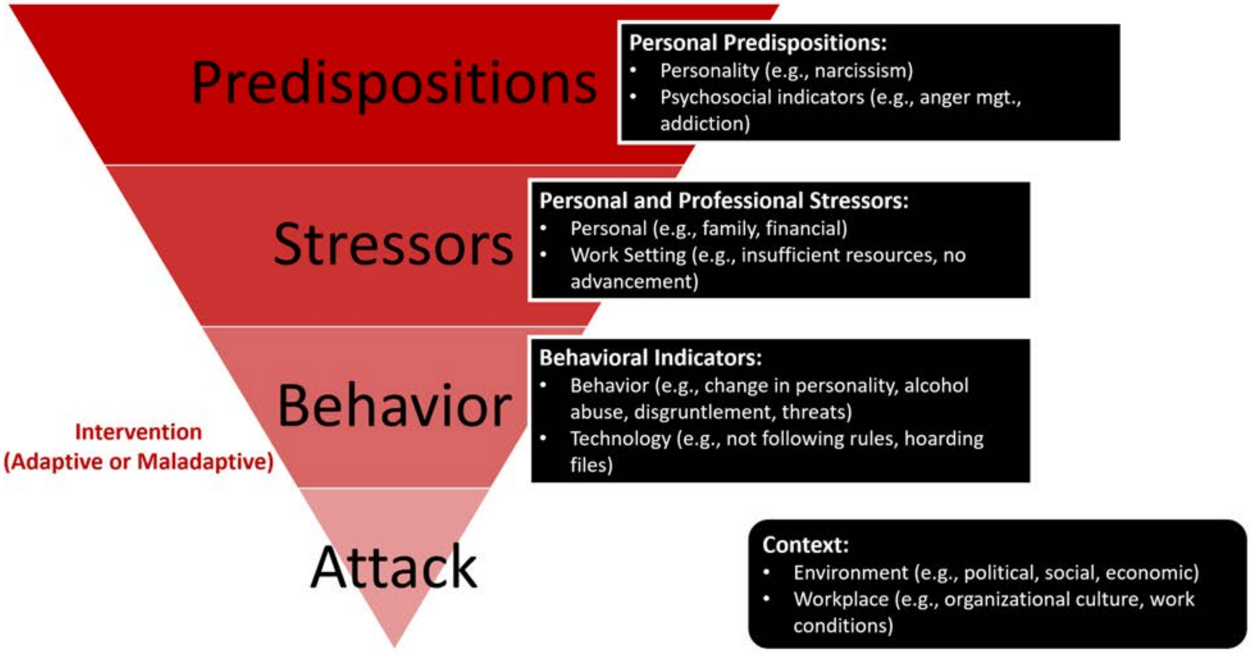

Predispositions
Personal Predispositions:
• Personality (e.g., narcissism)
• Psychosocial indicators (e.g., anger mgt., addiction)
Stressors
Personal and Professional Stressors:
• Personal (e.g., family, financial)
• Work Setting (e.g., insufficient resources, no advancement)
Behavior
Behavioral Indicators:
• Behavior (e.g., change in personality, alcohol abuse, disgruntlement, threats)
• Technology (e.g., not following rules, hoarding files)
Intervention
(Adaptive or Maladaptive)
Attack
Context:
• Environment (e.g., political, social, economic)
• Workplace (e.g., organizational culture, work conditions)

Figure 3. Graphical Representation of the Critical Pathway Model[7]

However, the critical path model is not without criticisms or limitations, as discussed recently by Lenzenweger and Shaw (2022). For example, empirical validation of the model remains limited (though efforts to collect data to bolster the evidence is underway), and questions remain regarding, among others, (a) methods empirically combining risk factors to develop risk profiles, (b) methods of "offboarding" individuals currently on the critical path, and (c) potential interactions among variables in the model. Despite these limitations, the critical pathway model remains foundational for those looking to understand the human element of insider threat risk.

Bedford and van der Laan (2020) describe several models of varying degrees of specificity, to include the critical path model pointing out that while earlier models focused on individual risk factors and technically-oriented solutions (e.g., access controls), recent models have sought to better capture the interplay between employees and their environment. Recognizing this, Predd and colleagues (2008) considered the role of the individual in the context of the organization (i.e., expressed policies), the system (i.e., implied policy), and the environment (e.g., economic). This attempts to situate threat events in a more contextual light, including whether an insider's actions were legal, the type of organizational policies in place, and the motives of the insider. Where these authors considered this issue from a high-level, others have examined the unique interactions of the some of the elements of this model more deeply.

For example, Greitzer and colleagues (2016; 2019; 2021) developed and validated (using expert judgment to inform Bayesian estimates) a comprehensive ontology for predicting insider threat risk. The hierarchical Sociotechnical and Organizational Factors for Insider Threat (SOFIT)

[7] Version of the model derived primarily from Noonan (2018).

ontology includes factors (individual, organizational), classes, subclasses, and observable indicators. For example, one of the classes within the individual factor is *job performance*, which can be further broken down into subclasses such as *cyberloafing* and *negative evaluation*. Within negative evaluation, for example, indicators might be *performance below expectation*, *complaints*, or *missed deadlines* (Greitzer et al., 2019). Similarly, Legg et al. (2013) proposed a conceptual model for insider threat detection with four categories of elements, including enterprise (e.g., organizational policies, business processes), people, technology and information, and physical (e.g., access controls, security surveillance). These models are notable for several reasons but are highlighted for our purposes because they (a) explicitly include organizational contextual factors, such as poor supervisor-employee relations or work conditions, in addition to individual and technical factors, and (b) are designed to help make predictions about the risk of a threat event.

Despite their strengths, the lack of external validation of these models is a key criticism from some authors, as is the observation that they can be difficult for practitioners to apply due to their complexity (Bedford & van der Laan, 2021; Schoenherr & Thompson, 2020). To address concerns about these and other models of insider threat, Schoenherr and Thomson (2020) proposed a model to differentiate employee actions and identify specific forms of insider threat. The model, SIEVE (severity, form of employee norm violation, intentionality, and ethicality), seeks to classify individual behaviors based on motivations to develop better monitoring and intervention frameworks. Nostro and colleagues (2014) also focus on motivations and opportunities of potential insiders by exploring the unique access that a given role may have and the attack pathways they may take. Sokolowski, Banks, Dover (2016) explore an agent-based model (i.e., how individuals interact with larger systems), but focus on the complex adaptive behavior of an individual, incorporating different motivations and organizational factors.

This set of complex intersecting factors has led to the development of integrated insider threat frameworks that go beyond traditional network monitoring and security procedures. For example, Bedford and van der Laan (2021) developed the Organizational Vulnerability to Intentional Insider Threat (OVIT) survey to describe factors that increase insider threat risk, with individual, organizational, and technical dimensions included. This model is notable because the derived measure can be used as a validation tool for evaluating new interventions. Whitty (2021), based on the coding of case studies derived from interviews with industry professionals, developed a model that incorporates practices such as hiring/pre-screening, improving the workplace culture, and so forth. This model is notable for its explicit inclusion of potential prevention factors. Finally, Elmrabit and colleagues (2020), building off Greitzer's work cited above, incorporate preventative factors into a detailed model of insider threat risk predictions. Graphical representations of all three models can be found in Appendix B.

Methods of Detecting Insider Threats

Techniques for detecting insiders are frequently classified into one of three categories—technical, non-technical, or a blend of the two (see Homoliak et al., 2019 for a more complete review). Early information security research recognized that technical solutions alone were insufficient for detecting and mitigating insider threat risk (e.g., Pfleeger & Caputo, 2011; Steele & Wargo, 2007). The methods of detection offered in the technical fields differ in their plans, implementation, and what they are hoping to capture. Most solutions end up being reactive, but there are some that try to be predictive. Some act as decision support systems to aid human judgment, while others are meant to operate largely autonomously.

A basic example of a technical solution is the proposition for a predictive system that flags those who are in the initial pathways of the insider threat cycle, specifically those that are accessing parts of the organization's computer system that they are not supposed to. These systems are based on permissions (are they supposed to be accessing this content) or expected job requirements (is accessing this content a normal part of their job). However, technical solutions can get more complex. For example, intrusion detection systems are deployed within a system to determine if there has been any intrusion from outside (Elmrabit et al., 2020). Intrusion detection can be executed in a number of ways. Artificial Neural Networks (ANNs) have been suggested as one solution, where a system will be trained to become familiar with normal work patterns and then be able to recognize and flag anything out of the norm (Williams et al., 2021).

In terms of non-technical solutions, common techniques include (a) policies (e.g., IT and HR policies), (b) personnel training (e.g., security awareness), and (c) psychological prediction (Elmrabit et al., 2020). "Psychological prediction" refers to characteristics that personnel around an insider will recognize and report. Maasberg et al. (2020), for example, has identified and empirically validated a set of observable behaviors associated with malicious insider threats. Bailey et al. (2018) discuss how HR and management could flag behavior from those they oversee and investigate as needed. Managers in this case need to be properly trained and have the time, resources, and familiarity with those they manage to be able to notice and flag concerning behavior.

Blended solutions combine policy and technical solutions, such as digital rights management, which can be seen in practices like deactivating work accounts and withdrawing credentials as soon as someone quits or is fired (Alawneh & Abbadi, 2011; Elmrabit et al., 2020; Silowash, 2013). Withdrawing credentials is just as important, if not more, for those that are working outside the organization (e.g., contractors) and have been given access to support the organization as they are an easy element to overlook. These contractors may not have a distinct termination moment, making it easy to forget to pull credentials. Another form of this digital rights management is group-based or role-based access control. These are systems that allow certain individuals or job roles (such as a systems administrator) to access specific files. This allows the narrowing of the scope of those who have access to the files, particularly if they are sensitive ones. This system helps protect critical files from modification, deletion, or unauthorized disclosure (Silowash, 2013).

We turn next to implications of this literature for the purpose of better understanding espionage, sabotage, and workplace violence from a threat assessment perspective.

Key Takeaways from Part 1

From the above literature review, we can conclude the following regarding the insider threat literature as it relates to threat assessment.

Takeaway 1: The insider threat literature includes detailed ontologies and testable, data-backed predictive models. Thus, these models can be very helpful in gaining a better understanding of the complex interplay of factors (e.g., personal predispositions, organizational, management actions, stressors) in support of threat assessment practice. For example, these models could help to enrich existing Structured Professional Judgment (SPJ) tools with (a) the identification of new indicators, (b) enhanced descriptions of existing indicators, or (c) data to inform potential weighting of indicators to support professional judgments.

However, as it relates to their application to threat assessment, these models are not without limitations. First, the level of specification of many of these models creates a challenge for non-technical professionals to use in a meaningful way to inform practice. This is not surprising given the field they came from—the complexity of these models is not a problem for machine-managed systems. However, translation will be required to help inform practice and policy. Second, most of the models of insider threat described above focus on "lone actors." Multi-actor threats are not considered in most of these models even though Whitty (2021) found 32% of insider threat cases in her study involved multiple actors. Most of the cases in this study were of fraud attacks, but the lack of consideration of multiple individuals working together is an oversight that should be built into any model. Finally, our literature review yielded very little information about the intersection between different types of security teams, such as cybersecurity, physical security, and other protective services. Better practices regarding the intersection of different security functions and related functions such as HR did emerge in our interviews with 13 threat assessment professionals (NCITE, 2022a), suggesting more work is needed.

Implications of takeaway 1: Insider threat models can be leveraged to inform threat assessment practice, but new literatures must be added to enhance applicability (e.g., the role that groups might play in insider threat). We address this implication in Part 2 by identifying other literatures that can build on current research related to insider threat.

Takeaway 2: Definitions of insider threat, even when narrowed to malicious insiders, includes a broad range of potential outcomes. As described above, early IS&T insider threat research focused narrowly on IT security violations. The expansion of the definition to capture other outcomes (e.g., fraud, workplace violence) requires corresponding enhancement of practice to consider off and on-network behaviors. Some indicators thought to be predictive of insider threat are, for a number of reasons, difficult to measure using network monitoring tools. For example, personal dispositions related to life events (e.g., marital problems) are not always easy to collect due to availability and/or ethical considerations. While HR and security technologies have increased employee monitoring capabilities, not all organizations will be comfortable with their use. Additionally, on-network indicators will be less relevant for certain types of organizations, such as mid-sized companies or companies where much of the work is done off network.

The range of outcomes and complexity in potential sources of data suggests more nuance may be needed in the models. The models referenced previously are designed to predict all types of outcomes, even though certain indicators may be highly relevant for certain outcomes and much less so than others. In reality, there may be multiple "pathways" to a threat event rather than one "critical" pathway. The idea of defining multiple pathways is not a new one. Lenzenweger and Shaw (2022), in discussing future directions of the original critical pathway model, suggest that identifying additional pathways would be a good enhancement of the original model. Whitty (2021) proposed several pathways to becoming an insider threat, such as "the addict," "pure greed," and "disgruntled employee." Finally, Shoenherr, Lilja-Lolax, and Gioe (2022), propose a multiple pathway approach to understanding social identities and motivations of threat actors that yields three general pathways: unintentional, ambivalent, and intentional.

Implications of takeaway 2: The forgoing suggests that, when considering models of espionage, sabotage, and workplace violence, it may be beneficial to start with a grounded theoretical approach that can be applied to a wide variety of contexts, with a particular emphasis on potential pathways.

Takeaway 3: Most proposed methods for mitigating insider threat risk focus on technical solutions to predict or catch an individual in an act of wrongdoing. Given the IS&T focus on network security, it is not surprising that the literature would emphasize technological solutions. However, as pointed out by others (e.g., Lang, 2022; Lenzenweger & Shaw, 2022), ideally mechanisms would be in place to *prevent* individuals from seriously considering an insider threat event in the first place (i.e., providing an "off-ramp" to those on the critical path). This could come in the form of deterrence or employee support strategies that add resilience to the system. While human and organizational factors feature prominently in the above-referenced models, they are treated primarily as data points to be used to inform risk profiles. There are opportunities to better leverage our understanding of these features in support of other, more preventative, policy initiatives, such as effective organizational leadership, codes of conduct, and employee assistance programs (Baweja et al., 2022).

Implication of takeaway 3: When considering insider threat mitigation (or reduction of insider threat risk), strategies to "positively deter" (Moore et al., 2016; 2022) or "off ramp" individuals from the critical path towards malicious activity should be explicitly incorporated into any recommendations. We discuss theoretical underpinnings of potential positive deterrence in Part 2.

Takeaway 4: The mechanism for applying general insider threat models to specific organizations is not always clear. Related to takeaway 2, it is not always readily apparent how the above-referenced insider threat models apply to specific organizational contexts. For example, the Greitzer et al. (2019; 2021) SOFIT model proposes specific indicators to be included in the model, but the specific metric/tool for populating that indicator is left to the organization. Implementation tools and guidelines are needed to bridge the gap between theory and practice. For example, the nature of the indicators, threat landscape, and types of people working in a specific job will depend on the job demand characteristics. Jobs can vary greatly on job context dimensions, such as degree of human interaction, physical work conditions, physical requirements, job hazards, degree of structure and responsibility, and so forth (Morgeson &

Humphrey, 2006). All of these may significantly impact (a) the manifestations of specific indicators and (b) their efficacy in predicting a threat event. Furthermore, it also changes the nature of potential malicious insiders themselves. To take an obvious example, kinetic workplace violence is unlikely to be a concern in a virtual financial services company, but fraud may be a significant concern. Certain fields also have specific demand characteristics, suggesting we would also expect to see differences in types of insider threat by discipline. Thus, comprehensive models of insider threat must also include mechanisms for "personalization" to the organizational context.

A final point related to this takeaway—assuming organizations do take action to mitigate potential insider threats, how can an organization determine whether it yielded a positive outcome? Because insider threat is a low base rate event, "absence of an incident" is not likely to be a particularly useful metric. This suggests the need to develop criterion measures for validating insider threat risk based on indicators—the goal of insider threat mitigation policies then would be to have a positive effect on these indicators. Bedford and van der Laan's (2021) OVIT survey provides a useful starting point in addressing this gap.

Implication of takeaway 4: When considering insider threat mitigation (or reduction of insider threat risk), strategies to contextualize general models to specific organizational contexts should be considered.

Part 2: Literatures Related to Insider Threat

As described in Part 1, most research classified specifically as “insider threat” comes from the information systems and technologies (IS&T) domain. However, other resources may also be brought to bear on the topic of insider threat as it relates to threat assessment. Our objective in this section is to gain a more complete understanding of insider threat antecedents and contextual factors from multiple perspectives. Thus, we distinguish among two types of resources in this section: (a) practitioner-oriented and (b) social and behavioral science. “Practitioner-oriented resources” refer to non-information security publications to assist professionals in a variety of domains (e.g., security professionals, managers, HR practitioners) in mitigating insider threat risk. In our review, we identified practitioner-focused resources for mitigating espionage, sabotage, and workplace violence. Next, relying on the authors’ individual expertise, we identified several social and behavioral science domains adjacent or related to the topic of insider threat. This includes political violence, preventing terrorism and targeted violence, counterproductive work behaviors, and organizational adaptability. For these sections, we relied on canonical articles to survey the literature and how each might be brought to bear on the topic of insider threat.

Practitioner-Oriented Resources

In the next three subsections, we describe practitioner-oriented resources for the three types of insider threats identified to be of most interest to the current context—espionage, sabotage, and workplace violence. We focus on practitioner-oriented resources as the academic literatures are touched on in other sections of the current report. This also helps to ground the remainder of the paper in the context of current best practice recommendations.

Espionage

Espionage is a subject that has captured the intrigue of the general public for decades—most notably in the decline of the Cold War, an era defined by escalating espionage capabilities between the United States and the USSR. However, espionage – i.e., spying – has changed dramatically in recent years. Organizations now face challenges of an increasingly cyber-connected world, with technology often moving faster than policymakers can keep up. This is commonly referred to as the “pacing problem,” first outlined by Larry Downes in his 2009 book *The Laws of Disruption* and with the now-famous quote: “technology changes exponentially, but social, economic, and legal systems change incrementally” (p. 2). One recent example of this problem emerging is in the use of facial recognition software. Despite widespread use by law enforcement and beyond, the entire state of California recently banned its use in police-worn body cameras (Merken, 2019). This demonstrates not only the inconsistent regulations of new technologies between states, but also exposes the fact that new technologies (such as facial recognition software on body cameras) are both available and widespread without any consistent regulations. In short, technology moves quickly and in unexpected ways, often leaving policymakers to play catchup. However, when the nature of the threat carries costs as high as insider threats can, organizational policies and mitigation strategies must remain current.

Early examinations of behavioral insider threats began with wanting to better understand espionage and its motivators. In many instances, espionage is perpetrated by insiders, as most cases of espionage involve those with access to protected knowledge, and thus are insiders by definition (*Insider Threat - Cyber | CISA*, n.d.). That is, when insiders steal information to benefit another organization or country, they are considered spies (*Data Loss Prevention*, 2019). Said simply, while not all insiders are spies, most spies are insiders, especially those who fall under the scope of classic espionage, described below.

While PERSEREC—the Defense Personnel and Security Research Center—was created in 1986 in the wake of the John Walker spy ring, the primary espionage statutes (Title 18 U.S.C. § 792-798), passed in 1917, have not changed since 1950 (Herbig, 2017).[8] However, espionage in practice has evolved dramatically since that time. The 1950 statute was written regarding the threat of the time, which, as described above, is generally now considered to be classic espionage. Classic espionage aligns more closely with the notions held by the public—that is, the idea of foreign actors who sneak their way into positions that provide them access to privileged information regarding our government, military, and other protected and secure private institutions.

Like most discussions that touch on acts of relevance to policymakers, we must first discuss what constitutes espionage in the real world. Espionage, in its simplest form, refers to spying. However, there are a range of forms of espionage, many of which diverge from our general conception of a spy infiltrating a protected agency, or *classic espionage*. A brief history of espionage in the United States helps us understand and distinguish between the various types of espionage, as well as the current state of (and responses to) espionage. This, in turn, informs our understanding of insider threats, as the origin of insider threats as a concept is born out of our efforts to counter and deter espionage efforts against us.

All forms of espionage, as a rule, involve the transfer of secret or protected information to another state entity, which is done covertly. While this typically involves the transfer to another state or other adversarial actors, in recent years, whistleblowers such as Edward Snowden have instead sought to release information to the public about their own government (referred to as "leakage"; CDSE *Insider Threat Awareness INT101.16*). [9] The various forms of espionage are outlined below.[10]

Types of Espionage

There is wide variation in types of espionage as well as an evolution of espionage more generally since the Cold War era. Classic espionage is formally defined as activities done for national government "A," which acts through an agent who clandestinely collects secrets from national government "B" that wants to control those secrets, and who turns them over to national government "A." (Herbig, 2017, p. 64). The classic spy also stands out as the "original

[8] It is worth noting that this statute, as well as preceding statutes that are frequently applied to espionage crimes, do not necessarily require transferred information to be classified.
[9] https://www.cdse.edu/Training/eLearning/INT101-signup/
[10] The Expanding Spectrum of Espionage by Americans, 1947 – 2015 Katherine L. Herbig, Ph.D.—Northrop Grumman Technology Services Released by—Eric L. Lang, Ph.D.

insider." That is, those who used deception to infiltrate secure facilities/organizations/personnel for the purpose of stealing information historically did so by becoming insiders (*Insider Threat - Cyber | CISA*, n.d.). They then abused their access as insiders to obtain secrets. Classic espionage usually involves theft of some sort, and generally requires an alternate identity, false flags, or other form of deceit. Definitions of classic espionage include: A Context of competition; Political, military, or economic secrets; Theft; Subterfuge and surveillance; Illegality; Psychological toll to the spy.

Classic espionage also covers acting as an agent of a foreign government. The FARA (Foreign Agent Registration Act) of 1938 is the primary way the U.S. federal government tracks these actors. Additionally, there is a parallel statute of the same name and year that primarily serves as the enforcement mechanism for failures to comply with the FARA. Potential offenses include clandestine operations, intelligence gathering, illegality, sabotage, terrorism, false identity, and the international proliferation of weapons of mass destruction. There have been increases in both registration and prosecutions over time, suggesting there are more foreign governments attempting to spy on the US than in previous years.

However, this "hands on" method of espionage is shifting toward more leaks and cyber espionage conducted directly by foreign powers. Classic espionage still exists and should not be discounted; however, the nature and mode of espionage have shifted dramatically since the Cold War era corresponding to developments in information technologies and geopolitical relations. In recent years, leaks of classified information have received more attention. Leaks are "disclosures of classified information to the public. They are usually accomplished through the press or by publication in print or electronic media. A leak often follows the form of classic espionage except that the recipient is different" (Herbig, 2017, p. 77). This is largely due to a number of high-profile leakers over the past decade in the US, such as Edward Snowden and Chelsea Manning. Leakers are generally not subject to whistleblower protections, but public support may vary depending on the nature of the leak. This was demonstrated by mixed public reactions in the fallout of the Snowden leak.[11] For leakers, "An additional controversial element in the debate about leaks is the tension between the need for government secrets and the First Amendment" (Herbig, 2017, p. 77). This also speaks to a need for reform of espionage statutes.

Finally, we must also consider economic espionage, which generally refers to theft of information by or for a foreign government and be a significant enough loss that it could have implications for the economy of the entire nation. "Industrial" and "corporate" espionage, in contrast, generally refers to theft from one company to another. While industrial and corporate espionage are typically domestic, these thefts may also have far-reaching economic implications. Trade secrets, often the target of corporate espionage, differ from classic espionage in that they don't involve classified information, but instead focus on the theft of privately owned intellectual property. The US Government has stated that, "it will not use the intelligence apparatus of the federal government to conduct economic espionage against other nations for the benefit of

[11] https://www.washingtonpost.com/opinions/was-snowden-hero-or-traitor-perhaps-a-little-of-both/2017/01/19/a2b8592e-c6f0-11e6-bf4b-2c064d32a4bf_story.html

American companies” (Herbig, 2017, p. 133). This distinguishes the US Government from other countries that do separate private entities from foreign governments.

The Economic Espionage Act (EEA) of 1996 was passed, in part, due to increases in the storage of information electronically, also illustrating the ways in which technology and information sharing has shifted our response to and understanding of espionage. Trade secrets don't have to be sold to foreign governments to qualify under this act—they simply must be going to a “foreign instrumentality,”[12] Further, violations of export control laws can be considered economic espionage if they include the sale, export, or re-transfer of various American defense articles and knowledge. This can include: military technologies and software, defense services, conventional weapons, missile technology, satellites, and nuclear, chemical, or biological materials and/or weapons (*U.S.C. Title 22 - FOREIGN RELATIONS AND INTERCOURSE*, 2010). The EEA was passed in 1996, but the underlying language assumes a Cold War context (Herbig, 2017). The dynamics of the global stage have changed significantly since then, with a range of potential nefarious foreign actors. There is general agreement among experts that these statutes need to be updated, but as of this writing, no agreement exists regarding how or in what direction. Ultimately, at its simplest level, the EEA is designed to protect technology that the US Government owns and does not want exposed.

As implied above, the nature of and trends in espionage have shifted dramatically alongside the increased use of IS&T. And while the advent of IS&T allows for many advantages for potential spies, it also potentially makes their actions more trackable than in previous generations. That is, IS&T follows everyone, including spies and leakers. As one observer noted, “A much bigger worry for spies is that the very vulnerabilities which make it easy for them to steal other people’s secrets also make it hard for them to hold on to their own” (Herbig, 2017, p. 158). This change has also resulted in the advent of cyber espionage by foreign governments. In this way, both the increase of IS&T and globalization stand out as a paradigm shift in the study and understanding of espionage and mass leakers. That is, federal entities like the US now have more adversaries, causing a range of potential entry points rather than one or a handful of nation-state adversaries.

Further changing the security landscape is economic globalization. Increasingly, large corporations operate in multiple countries, creating more opportunity for foreign intervention in those companies. Alternatively, increasing economic globalization has led to the hypothesis of greater cultural globalization. Cultural globalization could, in theory, decrease the risk of espionage due to alignment of economic interests, but increase the probability of individual violations in support of a “greater good.” This line of thinking has been used, in part, to explain the recent trend of mass leakers who release information for ideological reasons outside of providing information to an adversary or even financial gain (Thompson, 2018). Alongside a shift in the nature of espionage in the context of an increasingly interconnected world, the tempo of mass public disclosures, or mass leaks, appears to be increasing (Gioe & Hatfield, 2021). This is

[12] Foreign instrumentality: any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government (*Definition: Foreign Instrumentality from 18 USC § 1839(1) | LII / Legal Information Institute*, 1996)

occurring alongside the trend that departs from classic espionage and the Cold War paradigm, where actors are increasingly engaging in espionage activities without any influence from a foreign power or entity. Regardless of motivation, it is undeniable that we are in an increasingly interconnected world, both globally and electronically. As Gioe & Hatfield (2021) note:

> *"Even without such a verdict, however, the implications of trusted insiders with special system access privileges are profound, revealing the scope of the challenge for intelligence and security communities as well as their oversight bodies. Technology – in the early 21st century – favors the leaker from the inside and the hacker from the outside."* (p. 734).

Offender Characteristics

Herbig (2017) recently comprehensively summarized/analyzed decades of research and espionage case analysis on behalf of PERSEREC. Three cohorts are compared based on when the individual began espionage: 19471979, 1980-1989, and 1990-2015. Most of what we know about the characteristics of spies draws from these cohort studies.

Ultimately, there is no single profile for a spy or mass leaker. We do know some general characteristics, largely based off who has been charged with espionage in the past. Despite financial gains serving as a major motivating factor, those convicted of espionage are almost exclusively middle class (Thompson, 2014). However, we also know that financial motivations rarely stand alone as motivating factors. That is, there are undoubtedly many insiders with potentially highly valued access who do not turn to espionage as a means of financial gain. We also know from previous research that spies often have pathological personality features that may help separate them from their non-spy peers. That is, they are often thrill seekers, frequently exhibit narcissistic tendencies such as grandiosity, and desire power and control (Thompson, 2014; Wilder, 2017). Generally, these personality traits and their unique access can be seen as preconditions for espionage.

Another characteristic is the presence of some sort of critical triggering event that causes acute personal distress (Shaw & Sellers, 2015; Wilder, 2017). Past case analysis illustrates a range of triggering events that precipitated engagement in espionage (Herbig, 2017). This can include a sudden moral qualm, a personal grievance at the workplace, disgruntlement, economic hardship, or personal problems at home. The individual must then not only have access to protected information, but also a source willing to receive and reward that information. In the past, this typically referred to a foreign agent responsible for grooming and handling the spy. However, with mass leaking often referred to as the "new" espionage, the digital era allows for individuals to widely disseminate protected knowledge, such as in the Edward Snowden case. In these cases, a third party is not necessarily involved in either requesting or disseminating protected information. What remains less clear about this shift in behaviors is whether those engaging in mass leaking share different characteristics than those who fit the classic espionage profile. Personality traits associated with espionage include narcissism, psychopathy, and immaturity, while those associated with mass leaking often exhibit grandiosity, and are generally motivated by personal convictions or a concept of the "greater good" (Herbig, 2017; Thompson, 2014, 2018; Wilder, 2017).

The overwhelming majority of those convicted of espionage are middle class and male (Herbig, 2017). While a majority are white, this has been trending downward over time, with only 55% of the most recent cohort identifying as white. In general, those convicted of espionage are more likely to take risks or have committed crimes, and overall, the education level of spies is increasing over time. That is, individuals recently convicted of espionage have higher average levels of education than those convicted previously. In addition, the average age of those convicted of espionage is increasing. In short, "recent persons convicted of espionage-related offenses have been male, middle-aged, well-educated, and of a variety of racial and ethnic backgrounds that mirrors the increasing level of education and diversity of American society" (Herbig, 2017, p. 12). Another noteworthy trend in convicted spies is the increase in civilian convictions. The proportion of civilian spies increased from about 50% of all convictions to over 75% between two recent PERSEREC cohorts, corresponding with increased government contractor hiring in the post-9/11 era—a finding with potentially important policy implications.

Motivational Factors for Engaging in Espionage and Leaking

A prevailing theory of espionage engagement presents the conditions that must occur for a person to engage in espionage: (a) perceived opportunity, (b) contemplation of the act, (c) strong desire to obtain the likely outcomes of engaging in the act, (d) insufficient internal control mechanism, and (e) insufficient external controls. In theory, if one condition is not present, then espionage will not occur in that instance (Timm, 1991). However, this general model fails to adequately describe *why* an individual desires the outcomes of engaging in the act. The motivations for engaging in espionage generally fall in one of the following categories: economic, ideological, and disgruntlement/revenge. However, when analyzing cases, researchers find that there are often multiple motivations at play. Also, as described above, researchers are increasingly seeing individuals driven by personal beliefs who leak mass information to the public for the sake of fairness or "what's right." This is demonstrated by the motivational factors identified among PERSEREC's latest studied cohort of leakers:

- The leakers strongly objected to something they saw being done in the course of their work.
- The leakers enjoyed playing the role of expert.
- The leakers wanted to help and saw themselves as helping.

However, Thompson (2018) argues that mass leakers, along the lines of Snowden and Manning, represent a new type of "spy" altogether that require their own framework for understanding risk factors and motivations. He finds that the intersection of disgruntlement and narcissism are prominent features in mass leaking cases, which aligns with findings in espionage more generally. However, mass leakers are also motivated by a grandiose need for recognition. These motivations, combined with a media infrastructure that encourages a culture of "non-restraint" create the conditions for mass leaking. Similarly, Lillbacka (2017) argues that social context is an important consideration in understanding the motivations of spies and mass leakers. While it is generally regarded that "true" (that is, those motivated by ideology alone) ideologically motivated spies are a minority, ideology is a recurring theme across espionage cases.

Some with protected information have committed espionage due to the promise of extreme wealth or other dramatic returns in exchange for their insider knowledge. Others, like Snowden, claim purely altruistic or ideological purposes. However, these are not mutually exclusive. Rather, they can be seen as working together, alongside the conditions surrounding espionage. That is, if an insider is already disgruntled with their employer and receives an offer of financial gain in exchange for insider knowledge, and provided other necessary conditions are present, making the decision to leak or actively spy may be an easier one. Even among ideologically motivated leakers, there are often other motivational factors at play. For example, consider Jonathan Pollard, a U.S. Navy spy who sold state secrets to Israel. Despite receiving financial gains in return for secrets, he contends that his only motivation was to provide information to Israel. Further, he claims information sharing should have been occurring already, therefore he was "righting" an existing "wrong." While ideological motivations were likely a component of his espionage activities, the reality is that Pollard also received financial benefits in exchange for secrets, and so ideology is unlikely to stand alone as a motivator.

Sabotage

In addition to espionage, insider threat scholars and practitioners have classified sabotage as a major category of malicious insider behavior (Giacalone & Promislo, 2010; Greitzer et al., 2010; Kont et al., 2015; Theis et al., 2019). Whereas espionage entails gathering useful information to further the interests of parties *outside* the organization, the primary goal of sabotage is to interfere with and harm the processes and behaviors of those *inside* the organization (Giacalone & Promislo, 2010). Accordingly, sabotage involves intentionally impeding an organization's valued goals by withholding, tampering with, or destroying critical resources (e.g., information, tools, labor) that organization members rely on for their work (Analoui, 1995; Crino, 1994). The harm done by acts of sabotage generally occurs through process losses instead of direct psychological or physical damage (e.g., verbal aggression, workplace violence), but the form of sabotage varies based on the context, abilities, and motivations of deviant insiders (Ambrose, 2002; Greitzer et al., 2010; Liu et al., 2022; Schwepker Jr. & Dimitriou, 2022).

Common Forms of Sabotage

Research on organizational sabotage spans multiple disciplines including organizational behavior, hospitality management, risk and threat assessment, management information systems, and cybersecurity. Across these domains, scholars have examined four main classes of sabotage behaviors: production, service, knowledge, and IS&T. The many forms of sabotage represent insider threats to different organizational resources, vulnerabilities, and processes, and as such, pose distinct implications for prevention, detection, mitigation, and harm. Protecting organizational assets from sabotage thus requires a baseline understanding of the sources and types of sabotage behavior.

Production sabotage. Production sabotage refers to the deliberate slowing or halting of an organization's production processes (Hollinger & Clark, 1982). This type of sabotage tends to occur in work environments where employees' activities are interdependent (often sequential) and combine to yield material end-products (Saavedra et al., 1993; Taylor & Walton, 1971), such as assembly line manufacturing or R&D. Milder cases of production sabotage include production-slowing behaviors such as effort withholding, defying orders, or quitting. At more extreme levels, employees can disable production entirely through supply chain blockage, strikes, or destruction of machinery (Brown, 1977; Giacalone & Rosenfeld, 1987). Cases of production sabotage can cause substantial damage to an organization's tangible and intangible assets.

Service sabotage. Service sabotage involves behaviors of employees that are intended to undermine customer service and interests (Cheng et al., 2020). This form of sabotage can occur in any customer-facing role in service and hospitality industries. Examples of service sabotage include verbal hostility toward customers, delaying service, tampering with customer product orders, and deliberately failing to meet customer service requests (Harris & Ogbonna, 2006). The intentional interruption of customer service typically occurs at the direct expense of the customer, with indirect financial and reputational losses to the employer (Kao & Cheng, 2017; Liu et al., 2022).

Knowledge sabotage. Knowledge sabotage occurs when employees hide key work-related information or share false (i.e., misrepresented or fabricated) knowledge to mislead fellow workers and impede their ability to execute work tasks (Serenko, 2020). Much like service sabotage, knowledge sabotage occurs through interpersonal exchanges, but these behaviors differ in that knowledge sabotage targets co-workers more so than customers. Further, knowledge sabotage is distinct from benign cases of knowledge tampering such as white lies or unintentional knowledge hoarding, as the central aim of knowledge sabotage is to harm worker effectiveness and work processes (Connelly et al., 2012; Ferraris & Perotti, 2020). The severity of knowledge sabotage corresponds directly with the necessity of information for work-related processes and its exclusivity (i.e., the more critical and inaccessible the information is, the more harmful it is for one to withhold it).

IT sabotage. IT sabotage is broadly defined as an insider's malicious abuse of privileged IT system access to cause harm an organization and its members (Band et al., 2006; Greitzer, 2019). This can entail altering, hiding, or deleting important files (manually, or via installation of bugs and other rogue devices); fabricating information that mocks or damages the reputation of an organization; or disabling employees' access to electronic information, networks, or systems that are vital to conducting their work (Cappelli et al., 2012; Keeney et al., 2005). The outcomes of IT sabotage can range from operational impediments (e.g., halting of work and work processes, loss of time, increased employee workload) to reputational impairment (e.g., unfavorable perceptions from customers, distributors, suppliers, or other stakeholders) and financial loss (e.g., reduced production, loss of clientele, monetary cost of repairing damages). Additionally, IT sabotage can coincide with other forms of sabotage, as production machinery, personnel management software, customer support processes, and organizational data storage tend to be housed within IT systems.

Insider Motivations for Sabotage

Motivations for sabotage typically originate from self-interest and/or animosity toward an organization and its people (Serenko, 2020). More specifically, people enact sabotage behaviors when they seek to gain a competitive advantage over others at work or seek revenge for interpersonal or organizational grievances (Choo & Serenko, 2020; Crino, 1994; Gruys &

Sackett, 2003). Hiding valuable information from coworkers, for example, gives individuals near-exclusive access to necessary work-related information and places them in a position of relative power to others who must then rely on the knowledge holders (i.e., brokers) for information (Kwon et al., 2020; Perotti et al., 2022). Situations that fuel retaliatory acts of sabotage may include customer mistreatment (Liu et al., 2022; Scarlicki et al., 2008), interpersonal conflict at work (Eissa & Wyland, 2016), and frustration or ethical conflict with one's work and organization (Ambrose et al., 2002; Chen et al., 1992; Kont et al., 2015; Schwepker Jr. & Dimitriou, 2022). Taken together, most insider sabotage events generally arise from self-gratification or retribution motives, but the nature of actions taken hinges on the insider's access to critical organizational resources and capacity to thwart organizational processes.

Workplace Violence

Given high profile cases of kinetic violence, such as Nidal Hasan's terrorist attack on the Fort Hood installation, insider threat researchers have a significant interest in reducing risks from such violence in their workplace. However, in examining workplace violence scholarship and practice, definitional issues emerge in mapping that literature onto counter-insider threat research and practice. Specifically, researchers often distinguish between *workplace aggression* and *workplace violence*. Geck and colleagues (2017) define aggression as, "deliberate behavior by an employee who intended to or actually harmed another employee, with the emphasis being on psychological harm and not physical harm," and violence as, "workplace behavior that either inflicted physical harm or intended to inflict physical harm on another employee" (p. 211). Thus, the workplace violence literature uses a broader definition of violence than is frequently considered by insider threat researchers.

Scholars who study workplace violence further distinguish among four types of workplace violence that vary by the relationship between the perpetrator and the organization (e.g., CDC, 2004; CISA, 2019; and Geck et al., 2017):

1. **Criminal Intent**. In this type of workplace violence, the perpetrator has no legitimate relationship with the organization and is perpetuating violence as part of a criminal motive, such as robbery.
2. **Customer**. In this type of workplace violence, the perpetrator is a client, customer, student, or other similar status. Thus, the perpetrator has a legitimate relationship to the organization, but is not considered part of the organization.
3. **Employee**. This type of workplace violence is perpetrated by a current or former employee and would typically be considered an "insider threat."
4. **Personal Relationship**. In this type of workplace violence, the perpetrator has a relationship or association with someone in the organization, but not the organization itself. Often these are domestic disputes that carry over to the workplace context.

Workplace violence is rare and driven by occupational setting such that the first two types of workplace violence are most likely to occur in organizations that interface regularly with the public (Piquero et al., 2013). The Bureau of Justice Statistics (BJS), aggregating multiple nationally representative data sources, found the rate of nonfatal workplace violence to be 9.2 violent crimes per 1,000 workers (age 16 or older), with higher rates being observed in specific occupations such as mental health professionals (46.1 per 1,000), law enforcement officers (82.9 per 1,000), corrections officers (146.1 per 1,000), and bartenders (70.9 per 1,000) (Harrell et al., 2022; though it is widely agreed that workplace violence is underreported, see CDC, 2004). Because the incidence of workplace violence is skewed towards certain occupations, much of the literature focuses on risk factors and mitigation in certain domains (e.g., health care). Empirical literature specifically examining worker-to-worker workplace violence is rare, as it is far less prevalent than criminal and customer violence (Piquero et al., 2013). We summarize the relevant literature that is available next.

Workplace Violence Risk Factors

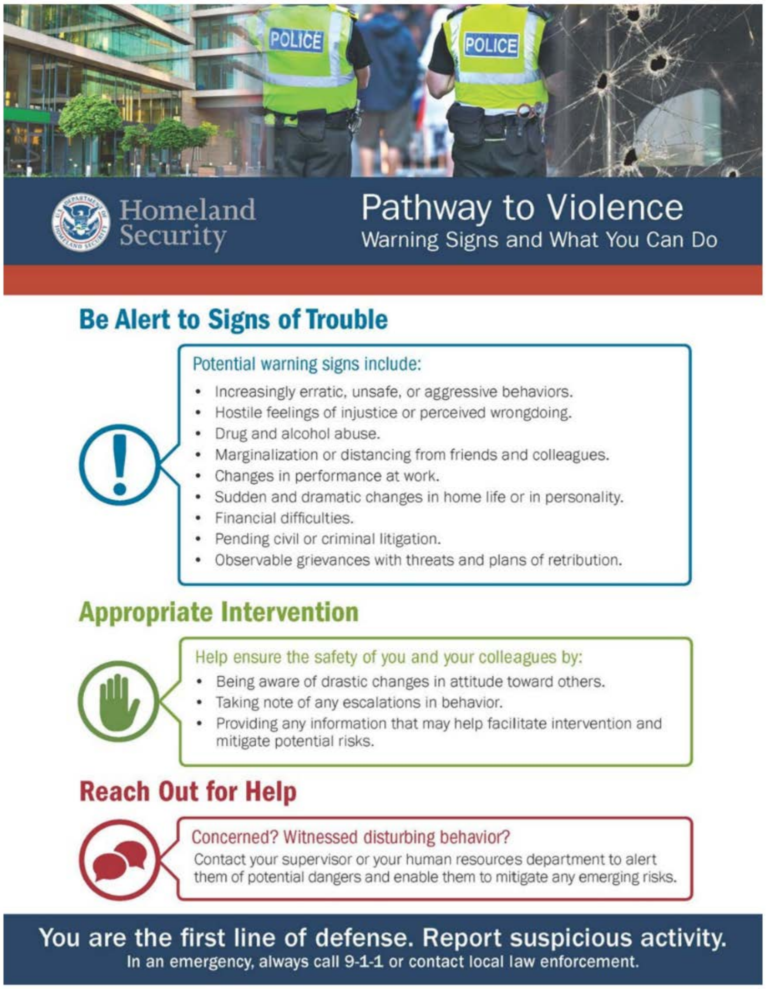
Given the wide variation by job, research and practice guides on identifying risk factors for workplace violence tend to focus on job and organizational characteristics. LeBlanc and Kelloway (2002) developed a job characteristics survey and found 22 items to be correlated with self-reported incidence of violence. These factors included job responsibilities (e.g., physical care of others, handle guns), context (e.g., work alone during the day), and customers (e.g., contact with individuals under the influence of alcohol). The Occupational Health and Safety Administration (OSHA, 2016), in their recommendations for the healthcare and social service sectors, identified additional risk factors associated with the organization or work setting, such as lack of staff training (lack of experience also comes up regularly as a risk factor in a review by Piquero et al., 2013), understaffing, high turnover, inadequate security, poor space design, and poor organizational processes. The Society for Human Resource Management (SHRM, 2023) also identifies "risky situations" in the workplace that may increase the risk of violence, including terminations and working with individuals with mental illness. Other problematic organizational responses (e.g., not taking indicators of risk seriously) are also likely to increase the probability of workplace violence or other negative outcomes (Lenzenweger & Shaw, 2022; Shaw & Sellars, 2015).

Geck and colleagues (2017) performed one of the few empirical studies examining individual risk factors for aggression and violence in a workplace setting. Building off an established set of eight risk factors associated with interpersonal violence,[13] the authors examined referrals to a workplace violence clinic and content coded the case files. In comparing violent to aggressive cases, they found that violent individuals were (a) more likely to have a marital status, potentially suggesting a spillover effect from home, (b) less likely to have been diagnosed with a mental illness, (c) less likely to have a history of threats, but more likely to have a history of violence in the workplace. In comparing one-time violent employees to those that were violent more than once, they found repeaters were more likely to have experienced physical abuse early in life, have a mental health diagnosis, and workplace histories of concerning behavior. Viñas-Racionero, Scalora, and Cawood (2021) used items from two Structured Professional Judgment (SPJ) to review 40 scenarios where individuals were exhibiting behaviors of concern. They found five indicators to be correlated at a statistically significant level with violent outcomes: (a) motives for violence, (b) homicidal fantasies/violent preoccupations, (c)

[13] Antisocial attitudes, antisocial associates, criminal history, antisocial personality factors, substance abuse, family factors, employment/school, and leisure/recreation (cf. Geck et al., 2017).

weapon skill/access/involvement, (d) preattack planning and preparation, and (e) suicidality/depression.

Other practitioner-focused resources emphasize proximal indicators of potential violence. For example, CISA provides a brochure of indicators for employers to be on the lookout for, such as "increasingly erratic, unsafe, or aggressive behaviors" and "sudden and dramatic changes in home life or in personality" (CISA, 2019; see Figure 4 for the full brochure and SHRM, 2023; OSHA, 2016 for additional examples). These indicators are consistent with some of the "concerning behaviors" described in the critical pathway model referenced previously (Lenzenweger & Shaw, 2022; Shaw & Sellars, 2015) as well as SPJ tools focused on workplace violence, such as the Workplace Assessment of Violence Risk (WAVR-21; White, 2021).



Homeland Security

Pathway to Violence
Warning Signs and What You Can Do

Be Alert to Signs of Trouble

Potential warning signs include:

- Increasingly erratic, unsafe, or aggressive behaviors.
- Hostile feelings of injustice or perceived wrongdoing.
- Drug and alcohol abuse.
- Marginalization or distancing from friends and colleagues.
- Changes in performance at work.
- Sudden and dramatic changes in home life or in personality.
- Financial difficulties.
- Pending civil or criminal litigation.
- Observable grievances with threats and plans of retribution.

Appropriate Intervention

Help ensure the safety of you and your colleagues by:

- Being aware of drastic changes in attitude toward others.
- Taking note of any escalations in behavior.
- Providing any information that may help facilitate intervention and mitigate potential risks.

Reach Out for Help

Concerned? Witnessed disturbing behavior?
Contact your supervisor or your human resources department to alert them of potential dangers and enable them to mitigate any emerging risks.

You are the first line of defense. Report suspicious activity.
In an emergency, always call 9-1-1 or contact local law enforcement.

Figure 4. "Pathway to Violence" Flyer[14]

Worker-on-Worker Violence Mitigation Strategies

[14] Source: https://www.cisa.gov/sites/default/files/publications/20_0210_cisa_isd_isc_workplace_violence_appendices.pdf (p. 25)

As it relates to insider threat, the practice guides referenced above tend to focus on two types of mitigation strategies: (a) removing barriers to workplace violence prevention strategies and (b) specific strategies for reducing the probability of worker-on-worker violence. With respect to the former, CDC (2004), for example, suggests organizations take workplace violence seriously by investing resources and committing to process improvements. Some suggestions for accomplishing these goals include, for example (CDC, 2004; CISA, 2019; OSHA, 2016), ensuing management and worker commitment; having a written workplace violence policy; establishing workplace violence prevention programs that includes a wide range of stakeholders (e.g., security, HR, legal, management); providing appropriate training to employees; and regularly reviewing, evaluating, and improving upon those programs. With respect to preventing worker-on-worker violence specifically, CISA (2019) provides the most comprehensive set of recommendations based on our review. While written to support workplace violence prevention efforts within the federal government, many of the recommendations generalize to other large organizations, including establishing:

1. *Screening processes to select out individuals at an elevated risk to commit violence*. This includes implementing pre-employment vetting processes (e.g., reference checks) and making use of probationary periods.
2. *Training programs to protect the workforce from potential violence*. This includes training for employees (e.g., on policies and procedures, as well as prevention strategies, such as anger and stress management), supervisors, and incident response teams.
3. *Alternative Dispute Resolution (ADR) programs*. ADR is an umbrella term for resolving disagreements through a neutral third party, such as ombudsmen, facilitation, and mediation.
4. *Incident response or threat assessment teams*. Summarizing current best practice for workplace threat assessment teams specifically is beyond the scope of the current section but is a critical element in workplace violence prevention.
5. *Employee Assistance Programs (EAPs)*. EAPs can be critical to early intervention efforts.
6. *Processes to help organizations recover after an incident*. This involves the identification of trained mental health professionals and the deployment of procedures (e.g., the Psychological First Aid model) to assist with recovery.

Social and Behavioral Science Perspectives

While the previous section described practitioner-focused perspectives, the next four subsections describe academic literature, at a high level, related to insider threat. Two of the sections – political violence and counterproductive work behaviors – provide foundational theoretical information and data that enhance how we understand insider threats. Specifically, the political violence literature addresses a gap identified in Part 1—the role that groups and/or ideology may play in insider threats. The literature on counterproductive work behaviors helps to enhance our understanding of potential antecedents and contextual factors that predict the maladaptive behaviors thought to be indicative of insider threat. The other two sections – preventing terrorism/targeted violence and adaptability – provide information that can be used in developing insider threat mitigation strategies. As the name implies, research into preventing terrorism and targeted violence examines community-based mitigation strategies of ideologically and non-ideologically motivated violence. We examine this literature to see if lessons may be learned for countering insider threats. Following on the general finding from Part 1 that disgruntled employees are far more likely to become insider threats, the adaptability literature provides a potential theoretical framework for avoiding negative employee outcomes (and enhancing positive outcomes) that increase insider threat risk.

Political Violence

With ideologically motivated insider threats, we turn to lessons from political violence to better understand the reasoning behind, for example, leaks and intellectual property thefts. In fact, many convicted spies explain that perceived immorality or they are engaging as a form of revenge against an agency (Thompson, 2018). Insiders pose a unique challenge for security professionals. They are uniquely positioned to cause more significant harms than average civilians who do not already have access to protected spaces and information. The distinction comes from their position within an organization, rather than any particular traits that are otherwise unique to other forms of criminals. In this sense, we can take the lessons learned from the targeted violence and political violence space. This area of research has sought to understand domestic violent extremism, whose attributes parallel those of insider threat. Although discussions about what constitutes domestic violent extremism (DVE) is contentious and nuanced in academic circles (Bennett & Lewis, 2022; Hoffman, 2017), we use it broadly here in reference to violent extremism and targeted violence between perpetrators and victims with the same citizenship. In its most basic sense, violent extremism refers to violence that occurs in the name of an extremist ideology, whereas targeted violence refers to acts of violence that are pre-planned and intentional – that is, that have a target in mind – but that are not motivated by political, ideological, or religious goals (McBride et al., 2021).

Recently, violent extremism and targeted violence have been formally recognized as internal threats to national security, prompting the United States government to release its first-ever National Strategy for Countering Domestic Terrorism (U.S. National Security Council, 2021). The current domestic violent extremist threat is further classified into two main threads: Anti-government or Anti-authority Violent Extremists (AGAAVE) and Racially and Ethnically Motivated Violent Extremism (REMVE). While there is substantive overlap, the former predominately targets institutions and other symbols of institutional authority (i.e., the Federal Government, police officers), whereas the latter focuses on violence targeted against individuals (i.e., members of a particular racial or ethnic group). These distinctions are intended to separate the motives behind violent acts, but the reality is that radical beliefs alone are not sufficient motives for violence (Asal et al., 2017; McCauley & Moskalenko, 2017; Wolfowicz et al., 2021). That is, radical beliefs alone are not a "conveyer belt" that leads ultimately to violent extremism. They may, however, be suggestive of how or at whom violence will be used, and when they exist alongside other risk factors, the likelihood of violence may increase.

Researchers are still working to understand what distinguishes those who engage in violence from other, nonviolent ideological extremists. However, what is increasingly clear is that it is not static factors that best predict risk of violence, but rather, dynamic ones. For example, fixed traits such as race, nationality, age, and sex are generally poor predictors of violence, regardless of an individual's level of extremism. Instead, the sociopolitical environments in which people are embedded, and their interactions with those environments, better serve to conceptualize domestic violence risk (Neo et al., 2017). For instance, while REMVE attackers have accounted for the majority of recent DVE attacks in the United States, AGAAVE attackers pose a greater risk to law enforcement and other authority figures resulting from situational interactions such as traffic stops (Clifford, 2021; "Strategic Intelligence Assessment and Data on Domestic Terrorism," 2021).

Such differences between these violent extremists suggest that discrete triggering events or contexts, in combination with one's beliefs, can increase the perceived viability and likelihood of violent behavior (Hamm & Spaaij, 2015). This parallels significantly with lessons from espionage, in that a triggering event aligns with opportunity and individual personality pathologies such as thrill-seeking behavior for an act of espionage to occur. Additionally, group norms and group membership can convince those with grievances and aggressive tendencies (or even those without, who join groups and movements out of social pressure or solidarity) to justify their mobilization toward violence for social and political aims (Asal et al., 2017; Clifford & Lewis, 2022). Thus, although radical beliefs are of concern, the foundations of violent actions are often *also* social or contextual in nature.

With that said, it is also worth noting that the dynamics around foreign actors and their role in espionage has evolved alongside technology. That is, after the Cold War, the dynamic began to shift to a threat of multiple state actors of ranging power, as opposed to one major superpower. In addition, actors working outside of the behest of a nation began to emerge. The increased reliance on IS&T has contributed to this shift by enabling outsiders access without needing to physically infiltrate a facility, such as in the case of cyberhackers who leak. While many hackers breach protected information to sell personal data for profit, others are ideologically motivated, and the two often intertwine. Take, for example, the hacktivist[15] group Anonymous. Most recently, Anonymous has been in the news for attacking Russian computer systems in protest of the 2022 Russian Invasion of Ukraine (*Russia-Ukraine War*, n.d.). However, Anonymous is not Ukrainian. Anonymous has no national identity, other than as a global collective that transcends global borders. Therefore, cyberattacks against the Russian state are in favor of one nation, but not acting on behalf of that nation. In addition, this is one of dozens of causes Anonymous has been involved in since its inception.

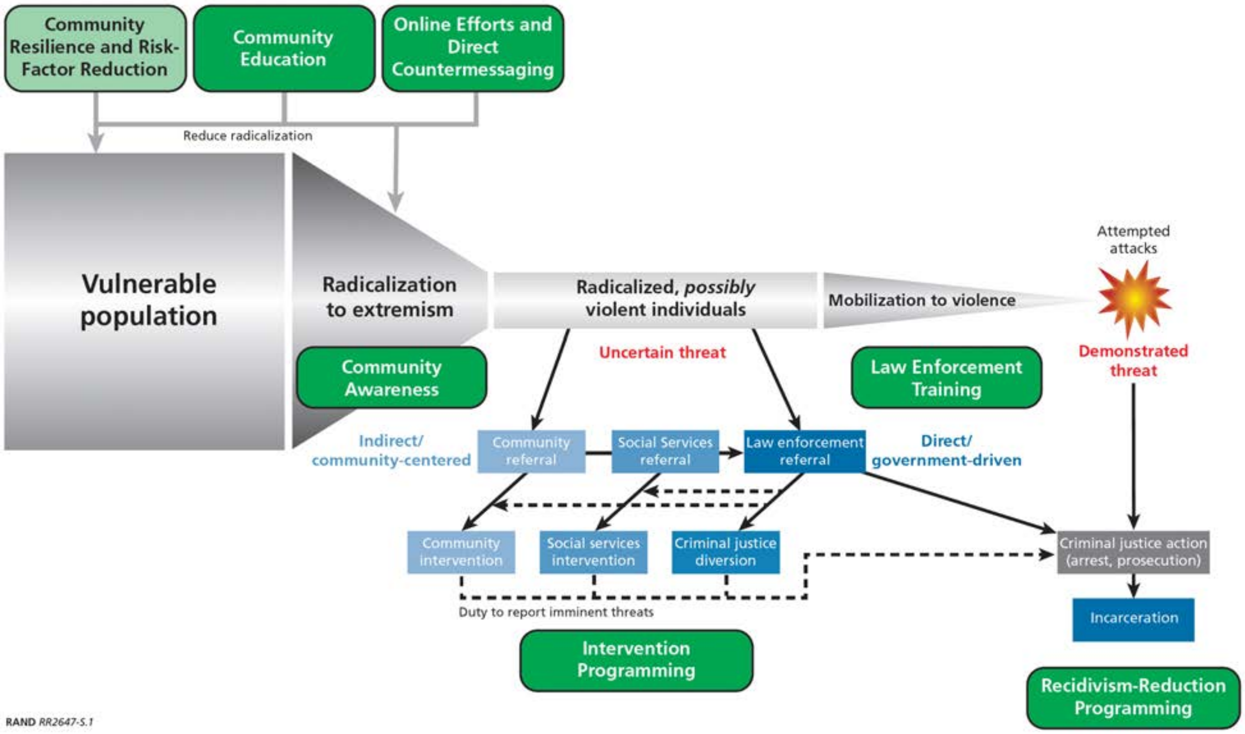
This is further demonstrated by massive leaking cases over the past decade committed by individuals with no allegiance to a particular nation or even, an extremist ideology. Consider the case of Edward Snowden. He leaked highly classified information as an American citizen while working for the National Security Agency (NSA) as a subcontractor. He was in no way working as a foreign actor or at the behest of an ideological group or even mission; rather, while working at the NSA, he claims that he became increasingly disillusioned, and that his formal disputes were ignored (*Snowden Speaks: A Vanity Fair Special Report | Vanity Fair*, n.d.). Cases like Snowden and Anonymous underly the shifting nature of both technology and an increasingly globalized world, as well as how they impact espionage and insider threats.

Terrorism and Targeted Violence Prevention

[15] Hacktivism-- Hacking to achieve social action or political objectives.

Recognizing ideologically motivated threats such as those described in the previous section, governments around the globe began in the early 2010's developing programs to counter terrorism from domestic sources. These programs, commonly known as "countering violent extremism" (CVE) programs in the academic literature, have several lines of effort and best practices associated with them (Stephens et al., 2021; NCITE, 2022b). In 2019, DHS published the *Strategic Framework for Countering Terrorism and Targeted Violence* that added targeted violence to domestic security concerns. The core difference between terrorism and targeted violence is perpetrators in the latter category lack "a clearly discernible political, ideological, or religious motivation," but both "are of such severity and magnitude as to suggest an intent to inflict a degree of mass injury, destruction, or death" (DHS, 2019; p. 4). Terrorism and targeted violence prevention then is a catch-all term for a wide variety of programming thought to prevent violence through non-criminal-justice-oriented means, such as programs to increase resilience (in both individuals and communities), countering narratives, disengagement programming, rehabilitation and reintegration, and so forth (Jackson et al., 2019; Sinai et al., 2019). Further, given the recency of these programs, challenges in community-based data collections, and the diversity of programming, there is a lack of empirical evidence to test targeted violence and terrorism prevention programs and associated underlying models (NCITE, 2022b; Sinai et al., 2019; Mastroe & Szmania, 2016).   Despite these limitations, we believe there is still value in surveying the state of this literature to determine whether any insights can be gleaned into insider threat research and practice.

With respect to theory, underlying CVE/counterterrorism programming is a "critical pathway"-type model that identifies vulnerable populations who start to become radicalized and eventually mobilize to violence. The RAND Corporation (Jackson et al., 2019), in a detailed review of the extant literature and interviews with subject matter experts of all types, developed the process model presented in Figure 4, which represents this underlying theory and maps DHS programming onto it. One can see much similarity with the Figure 3 presented previously, suggesting lessons learned in one field could potentially inform another. With respect to targeted violence, there is no one underlying theoretical model. McBride and colleagues (2022) present five potential underlying theoretical models, but synthesis is needed as theories often diverge greatly in their explanations of targeted violence. For example, the "Developmental Pathways to Demonstrative Targeted Attacks" theory suggests that perpetrators all follow a very similar pathway to targeted violence, while the "Intimate Massacres Model" theory suggests multiple pathways to violence.


Community Resilience and Risk-Factor Reduction
Community Education
Online Efforts and Direct Countermessaging
Reduce radicalization
Vulnerable population
Radicalization to extremism
Radicalized, *possibly* violent individuals
Mobilization to violence
Attempted attacks
Community Awareness
Uncertain threat
Law Enforcement Training
Demonstrated threat
Indirect/ community-centered
Community referral
Social Services referral
Law enforcement referral
Direct/ government-driven
Community intervention
Social services intervention
Criminal justice diversion
Criminal justice action (arrest, prosecution)
Duty to report imminent threats
Incarceration
Intervention Programming
Recidivism-Reduction Programming

RAND *RR2647-S.1*

Figure 5. Radicalization and Terrorism Prevention Framework (Jackson et al., 2019; p. xx)

Although these programs are still relatively new, enough work has been done around the world in the last 10+ years that summary reviews of available evidence have led to convergence on a few best practices that may find relevance to counter insider threat programming. We should also note that there is a lot of programming that is irrelevant to the insider threat context. To take an obvious example, recidivism reduction programs would not be in the purview of an individual organization. However, there are some transferrable lessons, the most relevant of which we describe below:

1. **Countering terrorism and targeted violence programs should be community-based.** A consistent recommendation among scholars in this space is that programming should be (a) community driven, where community leaders identify programming needs, and (b) highly customized to the needs of each individual community (Sinai et al., 2019, Jackson et al., 2019). It is an open question whether counter-insider threat programs should be similarly customized to organizations, a question we will explore in greater detail later in this paper.
2. **Emphasize community resilience.** Early CVE programming often focused on identifying communities "at risk" for terrorism, and developing programming geared toward a priori steering individuals away from violence. This led to feelings of marginalization by some community members and negative reactions (Jackson et al., 2019; Panduranga, 2021; Schanzer & Eyerman, 2019). This is similar to the backlash effects that can be found with heavy-handed security reactions to behaviors of concern in an insider threat

context (e.g., Moore et al., 2015; Shaw & Sellars, 2015). Programs that emphasize community resilience have the advantage of taking a strength versus a deficit-oriented perspective, which is more likely to be positively received, less prejudiced, and easier to evaluate (Stephens et al., 2021).

3. **Emphasize coordination and communication within communities.** Another aspect of resilience-focused programming is the need for real partnerships to develop between community organizations and government entities (Stephens et al., 2021). Having disparate groups work together from different perspectives on a common goal can be powerful. Additionally, effective targeted violence and terrorism prevention programs draw upon a wide range of disciplines, such as criminology, education, public health, and psychology (NCITE, 2022b; Stephens et al., 2021). All of this suggests that counter-insider threat should be a team sport, incorporating a variety of groups and disciplines that may include groups such as security, IT, HR, management, unions, and so forth.
4. **Build in program evaluation.** Given the newness of targeted violence and terrorism prevention programming, empirical evidence of the effectiveness of different programs is limited. Researchers have called for building evaluation into all programming to contribute to general knowledge regarding what works and does not (NCITE, 2022b). Similarly, organizations should also measure the return on investment in counter-insider threat programming. Programs that focus on resilience (which we describe as adaptability in the section below) are more likely to have positive benefits that go beyond the security-oriented needs.

Workplace Deviance and Counterproductive Work Behaviors

Organizational research on counterproductive work behaviors provides a direct picture of the individual, social, and contextual risk factors for harmful insider behaviors (INSA, 2017). Whereas political violence and preventing terrorism/targeted violence perspectives focus on extreme, outlier attitudes, intentions, and behaviors related to physical violence (Wolfowicz et al., 2021), scientific work on counterproductive work behaviors largely pertains to ordinary employees and their everyday discretionary, nonviolent activity (cf. LeBlanc & Kelloway, 2002; Neuman & Baron, 1998). In other words, harmful behaviors in organizations can unfold without extremist ideologies, radical intentions, or any interpersonal violence. Moreover, in comparison to political violence researchers, organization scholars emphasize the immediate social and organizational context more so than biographical data and life experiences (Gill et al., 2017; Simi et al., 2016). Harmful employee behaviors, through this perspective, are a product not only of individuals, but their interactions with others and reactions to organizational policies, practices, and procedures (Mackey et al., 2021). We provide a broad overview of this research area by describing the actions that fall within the umbrella of counterproductive work behaviors (and the targets of such behaviors), their common correlates, and implications for insider risk and threat assessment.

Definitions

Counterproductive work behaviors are defined as voluntary employee behaviors that reduce worker effectiveness and harm the organization's property, personnel, or functioning (Bennett et al., 2018). The definition of counterproductive workplace behaviors is similar to that of workplace deviance (i.e., voluntary employee behavior that violates organizational norms and harms the organization and its constituents), such that the terms are frequently used interchangeably (Carpenter & Berry, 2017). Although the differences are negligible, some researchers view workplace deviance as a subset of counterproductive behaviors that more explicitly violate norms (Mackey et al., 2021) because not all counterproductive work behaviors are non-normative (e.g., conflict with coworkers, withdrawal behaviors). For simplicity, however, we will use the broader term of counterproductive work behaviors.

Models of Counterproductive Work Behavior

There are three main empirical models that catalogue the structure of counterproductive work behaviors. Within these models, researchers primarily conceptualize counterproductive work behaviors by the *content* or *target* of behaviors (Marcus et al., 2016). Content refers to the types of specific work-related activities that fit within the definition of counterproductive work behaviors, and these behavior categories vary in their severity or potential for harm. In addition to behavior types, researchers also specify to whom or what such behaviors are targeted. These three models of counterproductive work behaviors are similar, yet distinct, as they differ in the extent that behavioral content and targets are represented. Below, we review the three models briefly and note their similarities and differences.

Bennett and Robinson (2000) provided one of the first measures of counterproductive work behaviors, based on their original conceptual typology of workplace deviance (Robinson & Bennett, 1995). This measure distinguishes between harmful behaviors targeted at individuals within the organization and actions targeted at the organization. The interpersonally oriented behaviors include forms of workplace aggression (Hershcovis, 2011), such as making racially insensitive remarks, cursing at someone, or publicly ridiculing someone at work. Behaviors that harm the organization include but are not limited to theft (of money, physical items, or time), disobedience, littering, on-the-job drug use, and lateness.

Gruys and Sackett (2003) developed what Marcus and colleagues (2016) described as the most comprehensive measure of counterproductive work behaviors. This measure organizes harmful behaviors by their content, which captures 11 behavior categories: (1) theft and theft-related behavior, (2) destruction of property, (3) misuse of information, (4) misuse of time and resources, (5) unsafe behavior, (6) poor attendance, (7) poor quality work, (8) alcohol use, (9) drug use, (10) inappropriate verbal actions, and (11) inappropriate physical actions. In contrast to Bennett and Robinson's (2000) measure, the behavior content categories capture a broader collection of workplace behaviors that encompass physical actions and harm. The measure by Gruys and Sackett (2003) does not explicitly group items by target, although it does distinguish interpersonally and organizationally directed behaviors.

Spector and colleagues (2006) created a five-facet model of counterproductive work behaviors that includes abuse, production deviance, sabotage, theft, and withdrawal. Much like Gruys and Sackett (2003), the researchers organized their items based on content rather than targets. However, their model development approach differed from Gruys and Sackett (2003) and Bennett and Robinson (2000) in that they used a theory-driven, rather than factor-analytic, approach to developing their facets (Marcus et al., 2016). Similar to Bennett and Robinson (2000), the measure represents narrower coverage of the counterproductive workplace behavior domain in comparison to Gruys and Sackett (2003). The model by Spector et al. (2006) can also be divided into interpersonally and organizationally directed behaviors, but most of their behavior content groupings target the organization, with the exception of abuse. Additionally, a distinguishing feature of this measure is that it excludes items related to substance abuse (argued by some scholars to be self-directed rather than organizationally directed behaviors; Marcus et al., 2016), which are present in the other two measurement models.

Despite the noted differences in facet structures and comprehensiveness, the behaviors represented within these three counterproductive workplace behavior models can generally be described via their content and targets. These models offer much direct utility to social scientific perspectives on insider threat. In particular, the content and targets of counterproductive work behaviors are crucial considerations for both research and practice because they give insight about how insider activities can manifest to harm an organization and its constituents. Modeling the content and structure of such behaviors, in other words, helps to identify potential behavioral indicators that predict insider threat. Although counterproductive work behaviors have been included in insider threat prediction and detection models (e.g., Bedford & van der Laan, 2021; Greitzer et al., 2018), research has also begun to recognize the importance of more distal antecedents of insider threat (Lenzenweger & Shaw, 2022), which are well-studied in the counterproductive work behavior literature. In fact, research on counterproductive work behaviors extends far beyond descriptive, definitional work and has examined a wealth of predictors such as personality traits, work stressors, attitudes, socio-organizational factors, and their interactions (e.g., Berry et al., 2007; Liao et al., 2021; Mackey et al., 2021). Advancing current insider threat risk models and assessment frameworks thus requires a deeper understanding of common antecedents of counterproductive work behaviors.

Correlates of Counterproductive Work Behaviors

A large body of research and meta-analyses on counterproductive work behaviors offer ample evidence for individual, social, and organizational factors that predict, or contribute to, employees' decisions to engage in detrimental workplace behaviors. Notably, research evidence indicates that personal and contextual factors can influence counterproductive work behaviors uniquely by themselves or jointly, in interaction with each other. Furthermore, different theories have been used to explain the occurrence of counterproductive work behaviors depending on the nature of the predictors. Here, we summarize the common correlates of counterproductive work behaviors and the theories that accompany them.

Individual factors. Individual worker characteristics that predict counterproductive work behaviors are mostly dispositional, but also include biographical data. In general, the strongest individual-level correlates of counterproductive work behaviors include personality traits reflective of less care about an organization, its work, and its people. Those with low agreeableness, conscientiousness, and emotional intelligence exhibit more counterproductive work behaviors (e.g., Bowling et al., 2011; Mackey et al., 2021; Zhou et al., 2014), as do people who score higher on measures of aggression (e.g., Galić & Ružojčić, 2017; Kranefeld & Blickle, 2022; Ružojčić et al., 2021; Runge et al., 2020) and Dark Triadic traits (i.e., psychopathy, Machiavellianism, narcissism; e.g., Ellen III et al., 2021; O'Boyle et al., 2012). More specifically, two recent meta-analyses found that conscientiousness (a task- and achievement-focused trait) was more strongly linked to counterproductive behaviors targeted toward the organization, whereas agreeableness (i.e., a socially oriented trait) was more strongly related to interpersonal aggression (e.g., Ellen III et al., 2021; Mackey et al., 2021). Moreover, a meta-analysis by Ellen III et al. (2021) determined that psychopathy and Machiavellianism were the strongest dark personality links to counterproductive work behaviors. Demographic variables are generally poor predictors of counterproductive work behaviors, but there is some evidence that biographical data such as history of aggression predicts aggressive interpersonal behaviors at work (Douglas & Martinko, 2001; Greenberg & Barling, 1999; Inness et al., 2005). Together, the individual-level predictors of counterproductive work behaviors are best explained by models of personality (e.g., Big Five, Dark Triad) and theories of aggression (Neuman & Baron, 1997), with stronger relationships between traits that match the nature of the target (e.g., conscientiousness is more strongly linked to carelessness at work and absenteeism than agreeableness).

Social factors. Extending beyond individual characteristics, counterproductive work behaviors can also arise from social experiences, such as deviant peers, experienced incivility, or the relationship between perpetrators and victims. Social explanations for counterproductive work behaviors are often rooted in social information processing or exchange theories (Bandura & Walters, 1977; Blau, 1964; Cropanzano & Mitchell, 2005; Salancik & Pfeffer, 1978). Through social learning and information processing, employees may feel pressure to model their deviant peers' behaviors at work (e.g., Azeem et al., 2021; Ferguson & Barry, 2011; Reynolds Kueny et al., 2020; Sakurai & Jex, 2012). In addition to social learning and pressures, counterproductive work behaviors can stem from anger and frustration that expected social exchanges at work are not met. Making rude remarks to a coworker, for example, may compel that coworker to retaliate or even pay that behavior forward to others (e.g., Hauge et al., 2009). Notably, these social exchanges are not limited to interpersonal conflict. In leader-follower relations, organizationally deviant follower behaviors (e.g., withdrawal, theft, poor job performance) can lead to interpersonally abusive supervision (e.g., yelling, belittling, undermining) and vice versa (e.g., Lian et al., 2014; Penney & Spector, 2005; Tepper et al., 2008; Wei & Si, 2013).

Work-related factors. Frustration from one's work or organizational practices, policies, and procedures can also motivate counterproductive work behaviors (INSA, 2017). Work- and organization-related correlates of counterproductive work behaviors usually involve issues of job strain and organizational justice, and they primarily result in harm toward the organization rather than its people. Work conditions that hinder, interfere with, or fail to support employees' accomplishment of work tasks tend to produce occupational stress and feelings of burnout (e.g., Fox et al., 2001; Meier & Spector, 2013; Penney & Spector, 2005). The resulting strain and job dissatisfaction from work-related constraints can lead employees to engage in counterproductive activity as a coping response, which can range from emotion-focused withdrawal (with little intent to change one's work conditions) to active resistance (Krischer et al., 2010; Shoss et al., 2016; Peter & O'Connor, 1980; Pindek & Spector, 2016). Similar effects have also been found for job insecurity and person-organization fit (Harold et al., 2016; Mackey et al., 2021). That is, job insecurity and perceptions of poor person-organization fit have been linked to increased expression of counterproductive work behaviors. Further, meta-analytic findings suggest that employees tend to respond adversely to perceived injustices at work, such as unfair pay, lack of informational transparency, inequitable procedures, and psychological contract breaches (Berry et al., 2007; Liao et al., 2021; Mackey et al., 2021). Employees who view their assigned work tasks as illegitimate or above their pay grade, for example, may refuse to do their work at all (Zhao et al., 2022).

Person × situation interactions. Although the individual, social, and work-related correlates of counterproductive behaviors do exhibit unique effects, organization scholars also recognize that such behaviors are influenced by a mixture of factors. That is, harmful insider behaviors are sometimes more likely to occur when personality traits interact with social and work-related factors. The effects of conscientiousness, agreeableness, and negative affectivity on counterproductive work behaviors, for instance, can be bolstered by negative work perceptions, ambiguity, and unfavorable interpersonal treatment (e.g., Colbert et al., 2004; Yang & Diefendorff, 2009). There is no shortage of potential person-by-situation interactions. What is crucial to note, though, is that situational factors can mitigate or exacerbate the effects of individual predictors. Since personality traits tend to have high stability, it is valuable to understand the influence of controllable, contextual factors (e.g., job characteristics, pay equity) that can be molded to subvert the risk of insider threat events.

Organizational Adaptability

In the inaugural issue of the journal *Counter Insider Threat: Research and Practice*, Moore, Gardner, and Rousseau (2022), following research conducted at SEI CERT (Moore et al., 2016), argue that insider threat mitigation programs can be augmented through *positive deterrence* strategies. Positive deterrence is defined in this paper as “workforce management practices that positively influence the organizational factors and result in reduced insider risk.” They contrast positive deterrence with the “command-and-control” tactics (e.g., security controls) typically relied upon for insider threat risk mitigation. Moore and colleagues further propose that heavy-handed command-and-control tactics may *increase* the probability of a threat event, suggesting there may be a limit to the amount of command-and-control procedures that an organization can implement before returns to security are diminished or even reversed. Indeed, scholars and practitioners have begun to recognize the importance of the “human dimension” in the context of security generally, and insider threats specifically (e.g., Greitzer, 2019; see also INSA, 2020 and CISA’s publication “HR’s Role in Preventing Insider Threats”[16]). As one illustration, Hobbs and Moran (2022), in their examination of nuclear-security system failures, illustrate that poor individual habits and workplace processes can neutralize even the best command-and-control security systems. As another example, studies have established the relationship between close antecedents to violence, such as workplace aggression, and poor leadership (Alhasnawi & Abbas, 2021; Hepworth & Towler, 2004).

[16] https://www.cisa.gov/sites/default/files/publications/HRs%20Role%20in%20Preventing%20Insider%20Threats%20Fact%20Sheet_508.pdf

In this section, following Dorsey, Allen, and Ingerick (2020), we propose that research on *organizational adaptability* may provide an underlying theoretical rationale identifying tools and techniques for (a) enhancing positive deterrence and (b) reacting swiftly and constructively to threat events. Specifically, organizational adaptability research may provide a mechanism for developing policies that act on factors considered to positively deter threat events. Organizational adaptability involves the study of how individuals and organizations respond to changing circumstances (see Baard et al., 2014 for a review).[17] Although there are many definitions, scholars generally agree that adaptability (a) has both proactive and reactive components (Griffen et al., 2007; Huang et al., 2014), (b) is context-dependent (Pulakos et al., 2000), and (c) is a "multi-level" phenomenon (Burke et al., 2006; Han & Williams, 2008). To elaborate:

a. **Proactive and reactive components.** In describing whether an individual is more or less "adaptable," the most comprehensive framework was developed by Pulakos and colleagues (2000; Dorsey et al., 2017), who identified eight dimension of adaptive performance (p. 617):
   1. Handling emergencies or crisis situations
   2. Handling work stress
   3. Solving problems creatively
   4. Dealing with uncertain and unpredictable work situations
   5. Learning work tasks, technologies, and procedures
   6. Demonstrating interpersonal adaptability
   7. Demonstrating cultural adaptability
   8. Demonstrating physically oriented adaptability

   These eight dimensions can be described as more proactive or reactive in orientation, such that, for example, "handling emergencies or crisis situations" can be described as an adaptive reaction to the environment, while "learning work tasks, technologies, and procedures" can be described as a proactive method of adapting to future requirements (Huang et al., 2014).

b. **Context dependence.** The specific nature of adaptation needed will depend on individual circumstances and the organizational context. For example, jobs with high physical requirements, such as with law enforcement or military personnel, are more likely to have a need for physically oriented adaptability, while those working in international contexts are more likely to require cultural adaptability. Thus, while there are antecedents and processes (described below) that will increase adaptability in general, the most effective adaptations are likely to be context specific.

c. **Adaptability as multi-level.** Since early work by Pulakos and colleagues (2000), scholars have begun to apply the concept of adaptability at the team and organizational levels (see, for example, Burke et al., 2006; Hatwig et al., 2020; Hillmann & Guenther, 2021; Maynard et al., 2015; Raetze et al., 2021; Stoverink et al., 2020). Multi-level models are

[17] When emphasizing different aspects of adaptability or particular domains, the terms "flexibility, "resilience," and "agility" are also used. For consistency, we use the term adaptability throughout this section.

common in social science research (e.g., Dansereau & Yammarino, 2003; Mumford & Hunter, 2005), recognizing that unique antecedents and processes are needed to describe effectiveness of the same concept at different levels. At these levels, adaptability is generally defined by measures of effectiveness in lieu of performance dimensions such as those described above. For example, team performance can be defined by a return to a baseline after an incident or change that impacts performance (cf. Burke et al., 2006; Hartwig et al., 2020). Team adaptation is also sometimes measured by member impressions of team adaptability, such as with a team adaptability scale developed by Marques-Qinteiro and colleagues (2015) that relies on the Pulakos et al. (2000) dimensions shown above. Similarly, organizational adaptability is frequently described by overall firm performance (e.g., Pulakos et al., 2019) or recovery from a disruptive event (Hillmann & Guenther, 2021).

We turn our attention now to factors that enhance adaptability at the individual and team levels. We focus on these two levels because they are most relevant to identifying potential positive deterrents to insider threat.

Antecedents of Adaptability

There is a substantial body of literature on antecedents of adaptability at all levels that can generally be classified in one of two ways. The first are *distal* antecedents indicative of adaptability that are stable/difficult to change without significant effort. The second are *process-focused* antecedents that are easier (relative to distal) to change and impact adaptability outcomes. These antecedents are not mutually exclusive—changes in processes can have a positive impact on distal antecedents for example. However, the distinction between distal and process-focused is useful for distinguishing variables to estimate baseline adaptability (distal) vs. driving new organizational policies to enhance adaptability (process-focused). As we examine the evidence for these antecedents at each level (individual, team), we find more empirical support for those identified at the individual than at the team level. We briefly summarize this research and implications below.

Individual-level factors. The distal and process-focused individual-level factors most likely to predict individual adaptability depend on the proactive and reactive components needed for the target job. For example, general mental ability (Dorsey et al., 2017), having a learning/mastery orientation (Bell & Kozlowski, 2008), and achievement striving (Griffin & Hesketh, 2005; Huang et al., 2014; Pulakos et al., 2002) are all thought to be distal predictors of adaptability. The primary mechanism for this relationship is through (a) the proactive process of learning new work tasks, technologies, and procedures; and (b) the ability to handle uncertain situations through learning. Similarly, knowledge (domain knowledge, broad knowledge, situational knowledge; Schmitt & Chan, 2006; Hunter et al., 2012; Mumford & Hunter, 2005) and openness to experience (Griffin et al., 2007; LePine et al., 2000) are also thought to be related to adaptability through research demonstrating their connection with solving problems creatively. The key takeaway from this literature is organizations that understand the adaptability demand characteristics of the roles within their organization are more likely to be able to select employees who are most likely to thrive in those roles.

In addition to these distal factors, there are process-focused actions that can be undertaken by individuals to increase their adaptability. For example, employees well trained on their technical tasks will have high (a) task knowledge and (b) self-efficacy (i.e., confidence in the ability to complete a task), both of which have been found to be related to adaptability in learning settings (e.g., Bell & Kozlowski, 2008). General positive attitudes and emotions are also predictive of adaptability (cf. Raetze et al., 2021), as are specific stress coping strategies, such as help-seeking behaviors (Britt et al., 2016). Organizational wellness programs, such as those that encourage healthy diet, sleep, exercise, and mindfulness habits are likely to have similar positive effects. These process-focused factors can be developed (e.g., through training) and encouraged (e.g., through policies and programs) by organizations to increase individual employee adaptability and, by extension, reduce the negative factors predictive of insider threats.

Team-level factors. Research into team level adaptability tends to focus on reactive forms of adaptability rather than proactive, with the notable exception of the robust literature on team creativity (Anderson, Potočnik, & Zhou, 2014; Mumford & Hunter, 2005). In reviews of team adaptability, the first factor generally considered critical to building capacity is team climate and culture. Scholarship supports two interrelated concepts as being important distal antecedents of adaptability—(a) psychological safety, or the ability for team members to speak up with without fear of reprisal (Ravishankar, 2022), and (b) continuous learning, or a culture that promotes reflection and development (Han & Williams, 2008). Similar to the role that learning/mastery orientation plays at the individual level, a continuous learning orientation at the team level is thought to improve team adaptability through knowledge acquisition by members, knowledge dissemination, and the ability to continuously update team mental models to solve problems (Han & Williams, 2008; Stoverink et al., 2020). Psychological safety is important during periods of uncertainty as open communication allows team members to make sense of the situation, plan, and take action (Burke et al., 2006; Stoverink et al., 2020).

This leads to another antecedent of team adaptability—team shared mental models, including the collective understanding of (a) tasks and resources needed to complete team objectives, (b) team member roles and responsibilities, and (c) team member knowledge, skills, strengths, and weaknesses (Mathieu et al., 2000). Shared mental models allow team members to quickly determine the next course of action in uncertain or unpredictable situations. Finally, team positivity and efficacy – the confidence that the team can address challenges – also help teams to better manage difficult or stressful situations (Raetze et al., 2021; Stoverink et al., 2020). In terms of processes, Burke and colleagues (2006) and Rosen and colleagues (2011) emphasize the criticality of planning behaviors in increasing team adaptability. This includes processes such as environmental scanning, developing effective plans, contingency/scenario planning, and taking deliberate steps to continuous improvement.

The underlying implication of the above section is, following propositions by Moore et al. (2022) and Dorsey et al. (2020), that adaptable individuals and teams are significantly less likely to generate an insider threat than less adaptable individuals and teams. The mechanism for this is positive deterrence—adaptable individuals and teams have positive outcomes (e.g., performance, commitment, wellness) even in adverse circumstances. If supported, this observation would have significant implications for addressing insider threats through policies that increase individual and team adaptability.

Key Takeaways from Part 2

From our review of the practitioner-oriented and social and behavioral science literatures in Part 2, we can take away the following as it applies to insider threat:

Takeaway 1: The practitioner-oriented literatures, in conjunction with the literature reviewed in Part 1, can deepen our understanding of malicious insider threat risk. The practitioner-oriented resources suggest some overlap and some unique indicators of threat across types. For example, the resources related to espionage, sabotage, and workplace violence all suggest the importance underlying grievance or disgruntlement and the presence of triggering events. However, as an example of a unique motivation, perpetrators of espionage (particularly leakers) are more likely, according to these literatures, to be driven by narcissistic tendencies, such as playing the role of an expert (Thompson, 2018), while perpetrators of workplace violence are more likely to be motivated by narcissistic injury, and turn to violence as a way to restore personal honor (White, 2021). This supports the "pathways" idea described in Part 1 (Lenzenweger & Shaw, 2022). An important implication of this observation is the potential that different counter-insider threat organizational policies or interventions could potentially be oriented towards different types of malicious insider threat.

Implication of takeaway 1: Models of insider threat should explicitly account for probability differences in risk indicators by types of malicious threat event.

Takeaway 2: The social and behavioral science literatures point to new potential methods for mitigating insider threat risk. Specifically, the political violence and terrorism/targeted violence literatures deepen our understanding of the role ideology and group membership can play in insider threat risk. This is critical as the role of these factors is under-represented in models of insider threat discussed in Part 1, and suggest new potential interventions, such as attention to engagements with AGAAVE and REMVE ideologies. The CWB and adaptability literatures both suggest organizational interventions that could be used to expand on the models presented in Part 1, and also suggest new interventions. For example, the adaptability literature suggests several potential avenues for increasing resilience at all organizational levels, providing potential positive deterrence factors against threat events. As a second example, both literatures point to the potentially crucial role of leadership in insider threat mitigation. Effective leadership at all levels improves a wide range of relevant outcomes, including lowering instances of CWBs, improving ethical behaviors, improving organizational climate and culture, and many others.

Implication of takeaway 2: Models of insider threat, and particularly positive deterrence counter-insider threat approaches, can be further informed by additional literature in the social and behavioral sciences.

Conclusions and Next Steps

The purpose of this report was to review extant literature related to insider threat to inform the larger threat assessment practice. In Part 1, we reviewed literature specifically related to insider threat, with a particular emphasis on the information systems and technologies (IS&T) field. We found that IS&T models of insider threat could be used to inform threat assessment research and practice. However, there were limitations to these models as they relate to threat assessment, such as less consideration of multi-actor threats, over-reliance on network-based indicators, and a lack of specificity in prevention-focused solutions. To address some of these limitations, we examined practitioner-oriented and behavioral and social science literatures related to insider threat. From the practitioner perspective, we learned that there are both overlapping and unique factors in the antecedents and situational factors predicting acts of espionage, sabotage, and workplace violence. From the social and behavioral science literatures, we learned that there are a variety of steps organizations can take to prevent threat events that are not currently well-specified in the literature.

The first two parts of this report are part of a larger effort to better understand insider threat and information threat assessment practice. Future work will add two more parts described below:

Future Part 3: Building Predictive Models of Workplace Violence, Espionage, and Sabotage. In this effort, we will systematically analyze the above literatures to better inform our understanding of workplace violence, espionage, and sabotage. We plan to accomplish this by leveraging systematic reviews (e.g., narrative reviews, meta-analyses, technical summaries) in each literature area from Parts 1 and 2 to build specified models, including proximal and distal antecedents and associated mediating and moderating relationships, of each threat type.

Future Part 4: Prevention-Focused Solutions. From the literature reviews and models from Future Part 3, we will offer a set of recommendations for potential solutions. Our recommendations will focus on early prevention interventions, as most of the extant literature in both counter-insider threat and threat assessment either (a) catch malicious behavior in the act (e.g., someone installing a backdoor for off-network access) or (b) involve late-stage preventions, such as intervening when someone exhibits behaviors of concern. Our goal is to develop solutions that inform policymakers and researchers in this space.

REFERENCES

Alawneh, M. & Abbadi, I. M. (2011). Defining and analyzing insiders and their threats in organizations. *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*. doi: 10.1109/TrustCom.2011.103

Alhasnawi, H. H., & Abbas, A. A. (2021). Narcissistic leadership and workplace deviance: A moderated mediation model of organizational aggression and workplace hostility. *Organizacija, 54*(4), 334-349. doi: 10.2478/orga-2021-0023

Althebyan, Q., & Panda, B. (2007). A knowledge-base model for insider threat prediction. *2007 IEEE SMC Information Assurance and Security Workshop*, 239–246. https://doi.org/10.1109/IAW.2007.381939

Ambrose, M. L., Seabright, M. A., & Schminke, M. (2002). Sabotage in the workplace: The role of organizational injustice. *Organizational Behavior and Human Decision Processes, 89*(1), 947–965. https://doi.org/10.1016/S0749-5978(02)00037-7

Analoui, F. (1995). Workplace sabotage: Its styles, motives and management. *The Journal of Management Development, 14*(7), 48–65. https://doi.org/10.1108/02621719510097361

Anderson, N., Potočnik, K., & Zhou, J. (2014). Innovation and creativity in organizations: A state-of-the-science review, prospective commentary, and guiding framework. *Journal of Management, 40*(5), 1297–1333. https://doi.org/10.1177/0149206314527128

Asal, V., Schulzke, M., & Pate, A. (2017). Why do some organizations kill while others do not: An examination of Middle Eastern organizations. *Foreign Policy Analysis*, *13*(4), 811-831. http://dx.doi.org/10.1111/fpa.12080

Azeem, M., Ahmed, M., Haider, S., & Sajjad, M. (2021). Expanding competitive advantage through organizational culture, knowledge sharing and organizational innovation. *Technology in Society, 66*, 101635. https://doi.org/10.1016/j.techsoc.2021.101635

Baard, S. K., Rench, T. A., & Kozlowski, S. W. (2014). Performance adaptation: A theoretical integration and review. *Journal of Management*, *40*(1), 48-99. https://doi.org/10.1177/01492063134882

Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2018). Insider threat: The human element of cyber-risk. *McKinsey & Company*. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/insider-threat-the-human-element-of-cyberrisk

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., & Trzeciak, R. F. (2006). *Comparing insider IT sabotage and espionage: A model-based analysis* (Technical Report CMU/SEI-2006-TR-026; p. 108). SEI CERT: Carnegie Mellon University.

Bandura, A., & Walters, R. H. (1977). *Social learning theory*. Prentice-Hall.

BaMaung, D., McIlhatton, D., MacDonald, M., & Beattie, R. (2018). The enemy within? The connection between insider threat and terrorism. *Studies in Conflict and Terrorism, 41*(2), 133–150. https://doi.org/10.1080/1057610X.2016.1249776

Baweja, J., Dunning, M. P., & Noonan, C. (2022). Domestic extremism: How to counter threats posed to critical assets. *Counter-Insider Threat Research and Practice*, *1*(1). https://citrap.scholasticahq.com/article/36185-domestic-extremism-how-to-counter-threats-posed-to-critical-assets

Bedford, J. & van der Laan, L. (2020). Operationalising a framework for organisational vulnerability to intentional insider threat: The OVIT as a valid and reliable diagnostic tool. *Journal of Risk Research*. DOI: 10.1080/13669877.2020.1806910

Bell, B. S., & Kozlowski, S. W. (2008). Active learning: Effects of core training design elements on self-regulatory processes, learning, and adaptability. *Journal of Applied psychology*, *93*(2), 296. https://doi.org/10.1037/0021-9010.93.2.296

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology, 85*(3), 349–360. https://doi.org/10.1037/0021-9010.85.3.349

Bennett, R. J., Marasi, S., & Locklear, L. (2018). Workplace deviance. *Oxford Research Encyclopedia of Business and Management.* Oxford University Press.

Bennett, C., & Lewis, J. (2022). *This is the aftermath*. Program on Extremism: The George Washington University.

Berry, C. M., Ones, D. S., & Sackett, P. R. (2007). Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology, 92*(2), 410–424. https://doi.org/10.1037/0021-9010.92.2.410

Bishop, M. & Gates, C. (2008). Developing strategies to meet the cyber security and information intelligence challenges ahead. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research*. doi: 10.1145/1413140.1413158

Bishop, M., Gollmann, D., Hunker, J., & Probst, C. W. (2005). Countering insider threats. *Dagstuhl Seminar Proceedings 08302,* 1-18. http://drops.dagstuhl.de/opus/volltexte/2008/1793

Blau, P.M. (1964) Justice in social exchange. *Sociological Inquiry, 34*, 193-206. http://dx.doi.org/10.1111/j.1475-682X.1964.tb00583.x

Bowling, N. A., Burns, G. N., Stewart, S. M., & Gruys, M. L. (2011). Conscientiousness and agreeableness as moderators of the relationship between neuroticism and counterproductive work behaviors: A constructive replication. *International Journal of Selection and Assessment*, *19*(3), 320-330. https://doi.org/10.1111/j.1468-2389.2011.00561.x

Britt, T. W., Shen, W., Sinclair, R. R., Grossman, M. R., & Klieger, D. M. (2016). How much do we really know about employee resilience? *Industrial and Organizational Psychology, 9*(2), 378-404. https://doi.org/10.1017/iop.2015.107

Brown, G. (1977). *Sabotage: a study in industrial conflict*. Bertrand Russell Peace Foundation for Spokesman Books.

Bulling, D., Scalora, M., Borum, R., Panuzio, J., & Donica, A. (2008). *Behavioral science guidelines for assessing insider threats* (7-2008). University of Nebraska Lincoln Public Policy Center. https://digitalcommons.unl.edu/publicpolicypublications/37

Burke, C. S., Stagl, K. C., Salas, E., Pierce, L., & Kendall, D. (2006). Understanding team adaptation: A conceptual analysis and model. *Journal of Applied Psychology*, *91*(6), 1189-1207. https://doi.org/10.1037/0021-9010.91.6.1189

Butts, J. W., Mills, R. F., Baldwin, R. O. (2005). Developing an insider threat model using functional decomposition. In V. Gorodetsky, I. Kotenko, & V. Skormin (Eds.), *Computer Network Security* (MMM-ACNS 2005). Lecture Notes in Computer Science (Vol. 3685). Springer: Berlin, Heidelberg. https://doi.org/10.1007/11560326_32

Cappelli, D., Moore, A. P., Trzeciak, R. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes*. Addison-Wesley Professional.

Carlson, A. (2020, August). *Combating insider threat with proper training*. Unpublished thesis.

Carpenter, N. C., & Berry, C. M. (2017). Are counterproductive work behavior and withdrawal empirically distinct? A meta-analytic investigation. *Journal of Management*, *43*(3), 834-863. https://doi.org/10.1177/01492063145447

Centers for Disease Control and Prevention (CDC) (2004, November). Workplace violence prevention strategies and research needs. Report from the conference *Partnering in Workplace Violence Prevention: Translating Research to Practice*. National Institute for Occupational Safety and Health (NIOSH): Baltimore, MD. Retrieved from https://www.cdc.gov/niosh/docs/2006-144/pdfs/2006-144.pdf?id=10.26616/NIOSHPUB2006144

Chen, P. Y. and Spector, P. E. (1992), Relationships of work stressors with aggression, withdrawal, theft and substance use: An exploratory study. *Journal of Occupational and Organizational Psychology, 65*, 177-184. https://doi.org/10.1111/j.2044-8325.1992.tb00495.x

Cheng, B., Guo, G., Tian, J. and Shaalan, A. (2020). Customer incivility and service sabotage in the hotel industry. *International Journal of Contemporary Hospitality Management,* 32(5), 1737-1754. https://doi.org/10.1108/IJCHM-06-2019-0545

Cybersecurity and Infrastructure Security Agency (CISA) (2019). *Violence in the federal workplace: A guide for prevention and response* (Version 4.0). Interagency Security Committee. Retrieved from https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide

Colbert, A. E., Mount, M. K., Harter, J. K., Witt, L. A., & Barrick, M. R. (2004). Interactive effects of personality and perceptions of the work situation on workplace deviance. *Journal of Applied Psychology, 89*(4), 599–609. https://doi.org/10.1037/0021-9010.89.4.599

Connelly, C. E., Zweig, D., Webster, J., & Trougakos, J. P. (2012). Knowledge hiding in organizations. *Journal of Organizational Behavior, 33*(1), 64–88. http://www.jstor.org/stable/41415737

Costa, D. L., Albrethsen, M. J., Collins, M. L., Perl, S. J., Silowash, G. J., & Spooner, D. L. (2016). *An Insider Threat Indicator Ontology* (Technical Report CMU/SEI-2016-TR-007; p. 87). SEI CERT: Carnegie Mellon University.

Crino, M. D. (1994). Employee sabotage: A random or preventable phenomenon? *Journal of Managerial Issues, 6*(3), 311–330.

Cropanzano, R., & Mitchell, M. (2005). Social Exchange Theory: An interdisciplinary review. *Journal of Management, 31,* 874-900. doi: 10.1177/0149206305279602

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology.* Advance online publication. https://doi.org/10.1007/s10869-021-09732-9

Definition: Foreign instrumentality from 18 USC § 1839(1) | LII / Legal Information Institute. (n.d.). Retrieved January 31, 2023, from https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=18-USC-1341432272-1439925515&term_occur=2&term_src=title:18:part:I:chapter:90:section:1839

Department of Homeland Security (2019, September). *Department of Homeland Security strategic framework for countering terrorism and targeted violence*. Retrieved from https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

Dorsey, D. W., Cortina, J. M., Allen, M. T., Waters, S. D., Green, J. P., & Luchman, J. (2017). Adaptive and citizenship-related behaviors at work (pp. 448-475). In J. L. Farr & N. T. Tippins (Eds.), *Handbook of Employee Selection, 2nd Ed*. Routledge.

Dorsey, D., Allen, M., & Ingerick, M. (2020, September). *Organizational adaptability: The next frontier for insider threat research*. Presentation to first annual Department of Defense (DoD) C-InT Social and Behavioral Sciences (SBS) Summit. https://sbssummit.com/

Douglas, S. C., & Martinko, M. J. (2001). Exploring the role of individual differences in the prediction of workplace aggression. *Journal of Applied Psychology, 86*(4), 547–559. https://doi.org/10.1037/0021-9010.86.4.547

Downes. (2009). The laws of disruption : harnessing the new forces that govern life and business in the digital age / Larry Downes. Basic Books.

Ellen, B. P. III, Alexander, K. C., Mackey, J. D., McAllister, C. P., & Carson, J. E. (2021). Portrait of a workplace deviant: A clearer picture of the Big Five and Dark Triad as predictors of workplace deviance. *Journal of Applied Psychology, 106*(12), 1950–1961. https://doi.org/10.1037/apl0000880

Elmrabit, N., Yang, S-H, Yang, L., & Yang, L. (2015). Insider threats in information security categories and approaches. *2015 21st International Conference on Automation and Computing (ICAC)*. doi:10.1109/IConAC.2015.7313979

Elmrabit, N., Yang, S-H, Yang, L., & Zhou, H. (2020). Insider threat risk prediction based on Bayesian network. *Computers & Security, 96*, 101908. https://doi.org/10.1016/j.cose.2020.101908

Ferguson, M., & Barry, B. (2011). I know what you did: The effects of interpersonal deviance on bystanders. *Journal of Occupational Health Psychology, 16*(1), 80–94. https://doi.org/10.1037/a0021708

Ferraris, A., & Perotti, F. A. (2020). Exploring the concept of "knowledge sabotage." *2020 IEEE International Conference on Technology Management, Operations and Decisions* (ICTMOD), 1–4. https://doi.org/10.1109/ICTMOD49425.2020.9380604

Fox, S., Spector, P. E., & Miles, D. (2001). Counterproductive work behavior (CWB) in response to job stressors and organizational justice: Some mediator and moderator tests for autonomy and emotions. *Journal of Vocational Behavior*, *59*(3), 291-309. https://doi.org/10.1006/jvbe.2001.1803

Galić, Z., & Ružojčić, M. (2017). Interaction between implicit aggression and dispositional self-control in explaining counterproductive work behaviors. *Personality and Individual Differences, 104*, 111–117. https://doi.org/10.1016/j.paid.2016.07.046

Geck, C. M., Grimbos, T., Siu, M., Klassen, P. E., & Seto, M. C. (2017). Violence at work: An examination of aggressive, violent, and repeatedly violent employees. *Journal of Threat Assessment and Management*, *4*(4), 210-229. https://doi.org/10.1037/tam0000091

Giacalone, R. A., & Rosenfeld, P. (1987). Reasons for employee sabotage in the workplace. *Journal of Business and Psychology, 1*(4), 367–378. https://doi.org/10.1007/BF01018145

Giacalone, R., & Promislo, M. (2010). Unethical and unwell: Decrements in well-being and unethical activity at work. *Journal of Business Ethics*, *91*(2), 275-297. https://doi.org/10.1007/s10551-009-0083-3

Gill, P., Silver, J., Horgan, J., & Corner, E. (2017). Shooting alone: The pre-attack experiences and behaviors of US solo mass murderers. *Journal of Forensic Sciences*, *62*(3), 710-714. https://doi.org/10.1111/1556-4029.13330

Gioe, D. V., & 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. https://doi.org/10.1080/09557571.2020.1853053

Greenberg, L., & Barling, J. (1999). Predicting employee aggression against coworkers, subordinates and supervisors: The roles of person behaviors and perceived workplace factors. *Journal of Organizational Behavior, 20*(6), 897–913. https://doi.org/10.1002/(SICI)1099-1379(199911)20:6<897::AID-JOB975>3.0.CO;2-Z

Greitzer, F. L., Kangas, L. J., Noonan, C. F., & Dalton, A. C. (2010, September). *Identifying at-risk employees: A behavioral model for predicting potential insider threats* (PNNL-19665). Pacific Northwest National Laboratory. https://doi.org/10.2172/1000159

Greitzer, F. L. (2019, April). Insider Threats: It's the HUMAN, stupid! *Northwest Cybersecurity Symposium*, ACM, Richland, WA. https://doi.org/10.1145/3332448.3332458

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation (pp. 85-113). In *Insider Threats in Cyber Security. Advances in Information Security, Vol. 49*. Springer.

Greitzer, F. L., Imran, M., Purl, J., Axelrad, E. T., Leong, Y. M., Becker, D.E., Laskey, K. B., & Sticha, P. J. (2016, November). Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk. *The Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security* (STIDS 2016), Fairfax, VA.

Greitzer, F. L., Purl, J., Becker, D. E., Sticha, P. J., & Leong, Y. M. (2019). *Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership*. Proceedings of the 52nd Hawaii International Conference on System Sciences.

Greitzer, F. L., Purl, J., Sticha, P. J., Yu, M. C., & Lee, J. (2021). Use of expert judgments to inform Bayesian models of insider threat risk. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 12*(2), 3-47. https://dx.doi.org/10.22667/JOWUA.2021.06.30.003

Griffin, B., & Hesketh, B. (2005). Are conscientious workers adaptable?. *Australian Journal of Management, 30*(2), 245-259. https://doi.org/10.1177/031289620503000204

Griffin, M. A., Neal, A., & Parker, S. K. (2007). A new model of work role performance: Positive behavior in uncertain and interdependent contexts. *Academy of management journal*, *50*(2), 327-347. https://doi.org/10.5465/amj.2007.24634438

Gruys, M. L., & Sackett, P. R. (2003). Investigating the dimensionality of counterproductive work behavior. *International Journal of Selection and Assessment, 11*(1), 30–42. https://doi.org/10.1111/1468-2389.00224

Han, T. Y., & Williams, K. J. (2008). Multilevel investigation of adaptive performance: Individual-and team-level relationships. *Group & Organization Management*, 33(6), 657-684. https://doi.org/10.1177/1059601108326799

Harold, C. M., Oh, I.-S., Holtz, B. C., Han, S., & Giacalone, R. A. (2016). Fit and frustration as drivers of targeted counterproductive work behaviors: A multifoci perspective. *Journal of Applied Psychology, 101*(11), 1513–1535. https://doi.org/10.1037/apl0000150

Harrell, E., Langton, L., Petosa, J., Pegula, S., Zak, M., Derk, S., Hartley, D., and Reichard, A. (2022). *Indicators of Workplace Violence, 2019* (NCJ 250748; NIOSH 2022-124). Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice; Bureau of Labor Statistics, Office of Safety, Health, and Working Conditions, U.S. Department of Labor; and National Institute for Occupational Safety and Health, Centers for Disease Control and Prevention, U.S. Department of Health and Human Services. Washington, DC.

Harris, L. C., & Ogbonna, E. (2006). Service sabotage: A study of antecedents and consequences. *Journal of the Academy of Marketing Science, 34*(4), 543–558. https://doi.org/10.1177/0092070306287324

Hartwig, A., Clarke, S., Johnson, S., & Willis, S. (2020). Workplace team resilience: A systematic review and conceptual development. *Organizational Psychology Review*, *10*(3-4), 169-200. https://doi.org/10.1177/2041386620919476

Hepworth, W., & Towler, A. (2004). The effects of individual differences and charismatic leadership on workplace aggression. *Journal of Occupational Health Psychology, 9*(2), 176–185. https://doi.org/10.1037/1076-8998.9.2.176

Herbig, K. L. (2017). *The Expanding Spectrum of Espionage by Americans, 1947-2015*. Defense Personnel and Security Research Center: Seaside, CA. https://apps.dtic.mil/sti/citations/AD1040851

Hershcovis, M. S. (2011). “Incivility, social undermining, bullying…oh my!”: A call to reconcile constructs within workplace aggression research. *Journal of Organizational Behavior, 32*(3), 499–519. https://doi.org/10.1002/job.689

Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research?. *International Journal of Management Reviews*, *23*(1), 7-44. https://doi.org/10.1111/ijmr.12239

Hobbs, C., & Moran, M. (2022). Exploring the human dimension of nuclear security: The history, theory, and practice of security culture. *Nonproliferation Review*. https://doi.org/10.1080/10736700.2020.1811532

Hoffman, B. (2017). *Inside Terrorism*. Columbia University Press.

Hollinger, R., & Clark, J. (1982) Employee deviance: A response to the perceived quality of the work experience. *Work and Occupations, 9*, 97-114. http://dx.doi.org/10.1177/0730888482009001006

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys, 52*(2), 30:1-30:40. https://doi.org/10.1145/3303771

Hou, T., & Wang, V. (2020). Industrial espionage – A systematic literature review (SLR). *Computers & Security*, *98*, 102019. https://doi.org/10.1016/j.cose.2020.102019

How Mobile Phones Became a Privacy Battleground—And How to Protect Yourself. (2022, September 29). *Wirecutter: Reviews for the Real World*. https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones/

Huang, J. L., Ryan, A. M., Zabel, K. L., & Palmer, A. (2014). Personality and adaptive performance at work: A meta-analytic investigation. *Journal of Applied Psychology, 99*, 162–179. https://doi.org/10.1037/a0034285

Hunter, S. T., Cushenbery, L., & Friedrich, T. (2012). Hiring an innovative workforce: A necessary yet uniquely challenging endeavor. *Human Resource Management Review, 22*(4), 303-322. https://doi.org/10.1016/j.hrmr.2012.01.001

IBM Security (2020). *Cost of insider threats: Global Report.* Accessed 1/27/2022 at https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/

Inness, M., Barling, J., & Turner, N. (2005). Understanding supervisor-targeted aggression: A within-person, between-jobs design. *Journal of Applied Psychology, 90*(4), 731–739. https://doi.org/10.1037/0021-9010.90.4.731

Insider Threat—Cyber | CISA. (n.d.). Retrieved January 30, 2023, from https://www.cisa.gov/insider-threat-cyber

Intelligence and National Security Alliance (INSA) (2017). *Assessing the mind of the malicious insider: Using behavioral model and data analytics to improve continuous evaluation*. Retrieved from https://www.insaonline.org/docs/default-source/uploadedfiles/2017/12/insa-wp-mind-insider-fin.pdf?sfvrsn=db23f48e_2

Intelligence and National Security Alliance (INSA) (2020). *Human resources and insider threat mitigation: A powerful pairing*. Retrieved from https://www.insaonline.org/docs/default-source/uploadedfiles/2020/01/insa-int-sept252020.pdf?sfvrsn=38fab99_2

Jackson, B. A., Rhoades, A. L., Reimer, J. R., Lander, N., Costello, K., & Beaghley, S. (2019). *Practical terrorism prevention: Reexamining U.S. national approaches to addressing the threat of ideologically motivated violence* (RR-2647-DHS). Homeland Security Operational Analysis Center (HSOAC): Rand Corporation.

Kao, F.-H., & Cheng, B.-S. (2017). Proservice or antiservice employee behaviors: A multilevel ethics perspective. *Human Performance, 30*(5), 272–290. https://doi.org/10.1080/08959285.2017.1399130

Keeney, Michelle & Kowalski, Eileen & Moore, Andrew & Shimeall, Timothy & Rogers, Stephanie. (2005). *Insider threat study: Computer system sabotage in critical infrastructure Sectors*. SEI CERT : Carnegie Mellon University.

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A. M. (2015). *Insider threat detection study*. NATO CCD COE, Tallinn. Retrieved from https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Kranefeld, I., & Blickle, G. (2022). Disentangling the relation between psychopathy and emotion recognition ability: A key to reduced workplace aggression? *Personality and Individual Differences, 184*, 111232. https://doi.org/10.1016/j.paid.2021.111232

Krischer, M. M., Penney, L. M., & Hunter, E. M. (2010). Can counterproductive work behaviors be productive? CWB as emotion-focused coping. *Journal of Occupational Health Psychology, 15*(2), 154–166. https://doi.org/10.1037/a0018349

Kwon, S. W., Rondi, E., Levin, D. Z., De Massis, A., & Brass, D. J. (2020). Network brokerage: An integrative review and future research agenda. *Journal of Management*, *46*(6), 1092-1120. https://doi.org/10.1177/0149206320914694

Lang, E. L. (2022). Seven (science-based) commandments for understanding and countering insider threats. *Counter-Insider Threat Research and Practice, 1*(1). https://citrap.scholasticahq.com/article/37321-seven-science-based-commandments-for-understanding-and-countering-insider-threats

LeBlanc, M. M., & Kelloway, E. K. (2002). Predictors and outcomes of workplace violence and aggression. *Journal of Applied Psychology, 87*(3), 444-453. https://doi.org/10.1037/0021-9010.87.3.444

Legg, P., Moffat, N., Nurse, J., Happa, J., Agrafiotis, I., Goldsmith, M., & Creese, S. (2013). Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4*, 20–37. http://doi.org/10.22667/JOWUA.2013.12.31.020

Lenzenweger, M. F., & Shaw, E. D. (2022). The critical pathway to insider risk model: Brief overview and future directions. *Counter-Insider Threat Research and Practice*, *1*(1). https://citrap.scholasticahq.com/article/36186-the-critical-pathway-to-insider-risk-model-brief-overview-and-future-directions

LePine, J. A., Colquitt, J. A., & Erez, A. (2000). Adaptability to changing task contexts: Effects of general cognitive ability, conscientiousness, and openness to experience. *Personnel Psychology, 53*(3), 563-593. https://doi.org/10.1111/j.1744-6570.2000.tb00214.x

Lian, H., Ferris, D. L., Morrison, R., & Brown, D. J. (2014). Blame it on the supervisor or the subordinate? Reciprocal relations between abusive supervision and organizational deviance. *Journal of Applied Psychology, 99*(4), 651–664. https://doi.org/10.1037/a0035498

Liao, Z., Lee, H. W., Johnson, R. E., Song, Z., & Liu, Y. (2021). Seeing from a short-term perspective: When and why daily abusive supervisor behavior yields functional and dysfunctional consequences. *Journal of Applied Psychology, 106*(3), 377–398. https://doi.org/10.1037/apl0000508

Lillbacka, R. (2017). The social context as a predictor of ideological motives for espionage. *International Journal of Intelligence and Counterintelligence*, *30*(1), 117–146. https://doi.org/10.1080/08850607.2016.1230704

Liu, M., Zhang, P., Gui, C., Lei, C., & Ji, X. (2022). Service sabotage in hospitality: A meta-analytic review. *Journal of Hospitality Marketing & Management, 31*(8), 984–1008. https://doi.org/10.1080/19368623.2022.2101169

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM, 63*(12), 64–80. doi: 10.1145/3408864

Mackey, J. D., Frieder, R. E., Brees, J. R., & Martinko, M. J. (2017). Abusive supervision: A meta-analysis and empirical review. *Journal of Management*, *43*(6), 1940-1965. https://doi.org/10.1177/014920631557399

Marcus, B., Taylor, O. A., Hastings, S. E., Sturm, A., & Weigelt, O. (2016). The structure of counterproductive work behavior: A review, a structural meta-analysis, and a primary study. *Journal of Management, 42*(1), 203–233. https://doi.org/10.1177/0149206313503019

Marques-Quinteiro, P., Ramos-Villagrasa, P. J., Passos, A. M., & Curral, L. (2015). Measuring adaptive performance in individuals and teams. *Team Performance Management*, *21*(7/8), 339-360. https://doi.org/10.1108/TPM-03-2015-0014

Mastroe, C., & Szmania, S. (2016, March). *Surveying CVE metrics in prevention, disengagement and deradicalization programs*. Report to the Office of University Programs, Science and Technology Directorate, Department of Homeland Security. College Park, MD: START.

Mathieu, J. E., Heffner, T. S., Goodwin, G. F., Salas, E., & Cannon-Bowers, J. A. (2000). The influence of shared mental models on team process and performance. *Journal of Applied Psychology, 85*(2), 273-283. https://doi.org/10.1037/0021-9010.85.2.273

Maynard, M. T., Kennedy, D. M., & Sommer, S. A. (2015). Team adaptation: A fifteen-year synthesis (1998–2013) and framework for how this literature needs to "adapt" going forward. *European Journal of Work and Organizational Psychology*, *24*(5), 652-677. https://doi.org/10.1080/1359432X.2014.1001376

McBride, M. K., Carroll, M., Mellea, J. L., Savoia, E. (2022). Targeted violence: A review of the literature on radicalization and mobilization. *Perspectives on Terrorism, 16*(2), 24-38. https://doi.org/10.31235/osf.io/nw672

Meier, L. L., & Spector, P. E. (2013). Reciprocal effects of work stressors and counterproductive work behavior: A five-wave longitudinal study. *Journal of Applied Psychology, 98*(3), 529–539. https://doi.org/10.1037/a0031732

Meloy, J. R., Hoffmann, J., Deisigner, E. R. D., & Hart, S. D. (2021). Threat assessment and threat management. In J. R. Meloy & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (pp. 3-21). Oxford University Press: New York.

Merken, S. (2019). *California Assembly OKs Facial Recognition Ban in Body Cameras*. Retrieved January 30, 2023, from https://news.bloomberglaw.com/privacy-and-data-security/california-assembly-oks-facial-recognition-ban-in-body-cameras

Moore, A. P., Gardner, C., & Rousseau, D. M. (2022). Reducing insider risk through positive deterrence. *Counter-Insider Threat Research and Practice*, *1*(1). https://citrap.scholasticahq.com/article/34612-reducing-insider-risk-through-positive-deterrence

Moore, A. P., Novak, W. E., Collins, M. L., Trzeciak, R. F., Theis, M. C. (2015). *Effective insider threat programs: Understanding and avoiding potential pitfalls* (DM-0001900). SEI CERT: Carnegie Mellon University.

Moore, A., Savinda, J., Monaco, E., Moyes, J., Rousseau, D., Perl, S., Cowley, J., Collins, M., Cassidy, T., VanHoudnos, N., Buttles-Valdez, P., Bauer, D., & Parshall, A. (2016). *The Critical Role of Positive Incentives for Reducing Insider Threats* (CMU/SEI-2016-TR-014). SEI CERT: Carnegie Mellon University.

Morgeson, F. P., & Humphrey, S. E. (2006). The Work Design Questionnaire (WDQ): Developing and validating a comprehensive measure for assessing job design and the nature of work. *Journal of Applied Psychology, 91*, 1321-1339. https://doi.org/10.1037/0021-9010.91.6.1321

Mumford, M. D., & Hunter, S. T. (2005). Innovation in organizations: A multi-level perspective on creativity (pp. 11-74). In F. J. Yammarino & F. Dansereau (Eds.), *Research in Multi-Level Issues*. Elsevier: Oxford.

National Counterterrorism, Innovation, Technology, and Education Center (NCITE) (2022b, March). *NCITE briefing on state of science in terrorism and targeted violence prevention efforts*. Briefing memorandum provided to the House Committee on Homeland Security. Omaha, NE.

National Counterterrorism, Innovation, Technology, and Education Center (NCITE) (2022a). *Threat assessment practitioner interviews*. Omaha, NE.

Neo, L. S., Dillon, L., & Khader, M. (2017). Identifying individuals at risk of being radicalised via the internet. *Security Journal*, *30*(4), 1112–1133. http://dx.doi.org.proxyau.wrlc.org/10.1057/s41284-016-0080-z

Neuman, J. H., & Baron, R. A. (1998). Workplace violence and workplace aggression: Evidence concerning specific forms, potential causes, and preferred targets. *Journal of Management, 24*(3), 391–419. https://doi.org/10.1016/S0149-2063(99)80066-X

Noonan, C. F. (2018, March). *Spy the lie: Detecting malicious insiders* (PNNL-SA-122655). Pacific Northwest National Laboratory: Oak Ridge, TN.

Nostro, N., Ceccarelli, A., Bondavalli, A., & Brancati, F. (2014). Insider threat assessment: A model-based methodology. *ACM SIGOPS Operating Systems Review, 48*(2), 3–12. https://doi.org/10.1145/2694737.2694740

O'Boyle, E. H., Jr., Forsyth, D. R., Banks, G. C., & McDaniel, M. A. (2012). A meta-analysis of the Dark Triad and work behavior: A social exchange perspective. *Journal of Applied Psychology, 97*(3), 557–579. https://doi.org/10.1037/a0025679

Occupational Safety and Health Administration (OSHA) (2016). *Guidelines for preventing workplace violence for healthcare and social service workers* (OSHA 3148-06R 2016). U.S. Department of Labor: OSHA. Retrieved from https://www.osha.gov/sites/default/files/publications/OSHA3148.pdf

Panduranga, H. (2021). *Community investment, not criminalization*. Brennan Center for Justice: New York University School of Law.

Penney, L. M., & Spector, P. E. (2005). Job stress, incivility, and counterproductive work behavior (CWB): The moderating role of negative affectivity. *Journal of Organizational Behavior, 26*(7), 777–796. https://doi.org/10.1002/job.336

Perotti, F. A., Ferraris, A., Candelo, E., & Busso, D. (2022). The dark side of knowledge sharing: Exploring “knowledge sabotage” and its antecedents. *Journal of Business Research, 141*, 422–432. https://doi.org/10.1016/j.jbusres.2021.11.033

Peters, L. H., O'Connor, E. J., & Rudolf, C. J. (1980). The behavioral and affective consequences of performance-relevant situational variables. *Organizational Behavior & Human Performance, 25*(1), 79–96. https://doi.org/10.1016/0030-5073(80)90026-4

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611. doi: 10.1016/j.cose.2011.12.010

Pindek, S., & Spector, P. E. (2016). Organizational constraints: A meta-analysis of a major stressor. *Work & Stress, 30*(1), 7–25. https://doi.org/10.1080/02678373.2015.1137376

Piquero, N. L., Piquero, A. R., Craig, J. M., & Clipper, S. J. (2013). Assessing research on workplace violence, 2000–2012. *Aggression and Violent Behavior, 18*(3), 383–394. https://doi.org/10.1016/j.avb.2013.03.001

Ponemon Institute (2022). *2022 Cost of insider threats global report*. Accessed 1/27/2022 at https://static.poder360.com.br/2022/01/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf

Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2008). Insiders behaving badly. *IEEE Security & Privacy, 6*(04), 66–70. https://doi.org/10.1109/MSP.2008.87

Pulakos, E. D., Arad, S., Donovan, M. A., & Plamondon, K. E. (2000). Adaptability in the workplace: Development of a taxonomy of adaptive performance. *Journal of Applied Psychology 85*(4), 612-624. https://doi.org/10.1037/0021-9010.85.4.612

Pulakos, E. D., Kantrowitz, T., & Schneider, B. (2019). What leads to organizational agility: It's not what you think. *Consulting Psychology Journal: Practice and Research, 71*(4), 305-320. https://doi.org/10.1037/cpb0000150

Pulakos, E. D., Schmitt, N., Dorsey, D. W., Arad, S., Borman, W. C., & Hedge, J. W. (2002). Predicting adaptive performance: Further tests of a model of adaptability. *Human Performance, 15*(4), 299-323. https://doi.org/10.1207/S15327043HUP1504_01

Raetze, S., Duchek, S., Maynard, M. T., & Kirkman, B. L. (2021). Resilience in organizations: An integrative multilevel review and editorial introduction. *Group & Organization Management*, *46*(4), 607-656. https://doi.org/10.1177/10596011211032129

Ravishankar, R. A. (2022). *A guide to building psychological safety on your team*. Harvard Business Review. https://hbr.org/2022/12/a-guide-to-building-psychological-safety-on-your-team

Reynolds Kueny, C. A., Francka, E., Shoss, M. K., Headrick, L., & Erb, K. (2020). Ripple effects of supervisor counterproductive work behavior directed at the organization: Using affective events theory to predict subordinates' decisions to enact CWB. *Human Performance, 33*(5), 355–377. https://doi.org/10.1080/08959285.2020.1791871

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal, 38*(2), 555–572. https://doi.org/10.5465/256693

Rosen, M. A., Bedwell, W. L., Wildman, J. L., Fritzsche, B. A., Salas, E., & Burke, C. S. (2011). Managing adaptive performance in teams: Guiding principles and behavioral markers for measurement. *Human Resource Management Review, 21*(2), 107-122. https://doi.org/10.1016/j.hrmr.2010.09.003

Runge, J. M., Lang, J. W. B., Zettler, I., & Lievens, F. (2020). Predicting counterproductive work behavior: Do implicit motives have incremental validity beyond explicit traits? *Journal of Research in Personality, 89*, 104019. https://doi.org/10.1016/j.jrp.2020.104019

Russia-Ukraine war: Anonymous hackers launch cyberwar against Russia taking down government websites. (n.d.). Business Insider. Retrieved January 31, 2023, from https://www.businessinsider.in/tech/news/russia-ukraine-war-anonymous-hackers-launch-cyberwar-against-russia-taking-down-government-websites/articleshow/89817168.cms

Ružojčić, M., Galić, Z., & Jerneić, Ž. (2021). How does implicit aggressiveness translate into counterproductive work behaviors? The role of job satisfaction and workplace anger. *International Journal of Selection and Assessment, 29*(2), 269–284. https://doi.org/10.1111/ijsa.12327

Saavedra, R., Earley, P. C., & Van Dyne, L. (1993). Complex interdependence in task-performing groups. *Journal of Applied Psychology, 78*(1), 61–72. https://doi.org/10.1037/0021-9010.78.1.61

Sakurai, K., & Jex, S. M. (2012). Coworker incivility and incivility targets' work effort and counterproductive work behaviors: The moderating role of supervisor social support. *Journal of Occupational Health Psychology, 17*(2), 150–161. https://doi.org/10.1037/a0027350

Salancik, G. R., & Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. *Administrative Science Quarterly, 23*(2), 224–253. https://doi.org/10.2307/2392563

Skarlicki, D. P., van Jaarsveld, D. D., & Walker, D. D. (2008). Getting even for customer mistreatment: The role of moral identity in the relationship between customer interpersonal injustice and employee sabotage. *Journal of Applied Psychology, 93*(6), 1335–1347. https://doi.org/10.1037/a0012704

Schanzer, D., & Eyerman, J. (2019, August). *Engaging with communities to prevent violent extremism: A review of the Obama administration's CVE initiative* (Document No. 256018). Office of Justice Programs.

Schmitt, N., & Chan, D. (2006). Situational judgment tests: Method or construct? In J. Weekley & R. E. Ployhart (Eds.), *Situational judgment tests* (pp.135–156). Mahwah, NJ: Lawrence Erlbaum.

Schoenherr, J. R., & Thomson, R. (2020, June). Insider threat detection: A solution in search of a problem. *In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-7). IEEE.

Schoenherr, J. R., Lilja-Lolax, K., & 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). https://citrap.scholasticahq.com/article/37117-multiple-approach-paths-to-insider-threat-map-it-intentional-ambivalent-and-unintentional-insider-threats

Schwepker, C. H., & Dimitriou, C. K. (2022). Reducing service sabotage: The influence of supervisor social undermining, job stress, turnover intention and ethical conflict. *Journal of Marketing Theory and Practice*. https://doi.org/10.1080/10696679.2022.2080713

Serenko, A., & Choo, C. W. (2020). Knowledge sabotage as an extreme form of counterproductive knowledge behavior: The role of narcissism, Machiavellianism, psychopathy, and competitiveness. *Journal of Knowledge Management, 24*(9), 2299–2325. https://doi.org/10.1108/JKM-06-2020-0416

Shaw, E. D., & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. *Studies in Intelligence, 59*(2), 41-48. The Central Intelligence Agency: Washington, DC.

Shoss, M. K., Jundt, D. K., Kobler, A., & Reynolds, C. (2016). Doing bad to feel better? An investigation of within- and between-person perceptions of counterproductive work behavior as a coping tactic. *Journal of Business Ethics, 137*(3), 571–587. https://doi.org/10.1007/s10551-015-2573-9

Society for Human Resource Management (SHRM) (2023). *Understanding workplace violence prevention and response*. Website URL: https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplace-violence-prevention-and-response.aspx

Silowash, G. J. (2013). *Insider threat attributes and mitigation strategies* (CMU/SEI-2013-TN-018). SEI CERT: Carnegie Mellon University.

Simi, P., Sporer, K., & Bubolz, B. F. (2016). Narratives of childhood adversity and adolescent misconduct as precursors to violent extremism: A life-course criminological approach. *Journal of Research in Crime and Delinquency, 53*(4), 536–563. https://doi.org/10.1177/0022427815627312

Sinai, J., Fuller, J., & Seal, T. (2019). Effectiveness in counter-terrorism and countering violent extremism. *Perspectives on Terrorism*, *13*(6), 90-108.

Snowden Speaks: A Vanity Fair Special Report | Vanity Fair. (n.d.). Retrieved January 31, 2023, from https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview

Sokolowski, J. A., Banks, C. M., & Dover, T. J. (2016). An agent-based approach to modeling insider threat. *Computational and Mathematical Organization Theory, 22*(3), 273–287. https://doi.org/10.1007/s10588-016-9220-6

Spector, P. E., Fox, S., Penney, L. M., Bruursema, K., Goh, A., & Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviors created equal? *Journal of Vocational Behavior, 68*(3), 446–460. https://doi.org/10.1016/j.jvb.2005.10.005

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security, 16*(1), 23–33. https://doi.org/10.1080/10658980601051334

Stephens, W., Sieckelinck, S., & Boutellier, H. (2021). Preventing violent extremism: A review of the literature. *Studies in Conflict & Terrorism, 44*(4), 346-361. https://doi.org/10.1080/1057610X.2018.1543144

Stoverink, A. C., Kirkman, B. L., Mistry, S., & Rosen, B. (2020). Bouncing back together: Toward a theoretical model of work team resilience. *Academy of Management Review*, *45*(2), 395-422. https://doi.org/10.5465/amr.2017.0005

Taylor, L., & Walton, P. (1971). Industrial sabotage: Motives and meanings. In S. Cohen (Ed.), *Images of Deviance* (pp. 219-245). Harmondsworth, England: Penguin.

Tepper, B., Henle, C., Lambert, L., Giacalone, R., & Duffy, M. (2008). Abusive supervision and subordinates' organization deviance. *The Journal of Applied Psychology, 93*, 721–732. https://doi.org/10.1037/0021-9010.93.4.721

Theis, M. C., Trzeciak, R. F., Costa, D. L., Moore, A. P., Miller, S., Cassidy, T., & Claycomb, W. R. (2019, February). *Common sense guide to mitigating insider threats* (6th ed.) (CMU/SEI-2018-TR-010). SEI CERT: Carnegie Mellon University. http://doi.org/10.1184/R1/12363665.v1

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472–484. https://doi.org/10.1016/j.cose.2005.05.002

Thompson, T. J. (2014). Toward an updated understanding of espionage motivation. *International Journal of Intelligence and Counterintelligence*, *27*(1), 58–72. https://doi.org/10.1080/08850607.2014.842805

Thompson, T. J. (2018). A psycho-social motivational theory of mass leaking. *International Journal of Intelligence and Counterintelligence*, *31*(1), 116–125. https://doi.org/10.1080/08850607.2017.1374800

Timm, H. W. (1991). Information security: Who will spy? *Security Management*, *35*(7), 49-53.

U.S.C. Title 22—FOREIGN RELATIONS AND INTERCOURSE. (n.d.). Retrieved January 31, 2023, from https://www.govinfo.gov/content/pkg/USCODE-2010-title22/html/USCODE-2010-title22-chap39.htm

Viñas-Racionero, R., Scalora, M. J., & Cawood, J. S. (2021). Workplace violence risk instrumentation: Use of the WAVR-21 V3 and the CAG (pp. 522-535). In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd Edition). Oxford Academic. https://doi.org/10.1093/med-psych/9780190940164.003.0030

Wei, F., & Si, S. (2013). Tit for tat? Abusive supervision and counterproductive work behaviors: The moderating effects of locus of control and perceived mobility. *Asia Pacific Journal of Management, 30*(1), 281–296. https://doi.org/10.1007/s10490-011-9251-y

White, S. G. (2021). Workplace targeted violence: Assessment and management in dynamic contexts (pp. 107-135). In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd Edition). Oxford Academic. https://doi.org/10.1093/med-psych/9780190940164.003.0006

Whitty, M. T. (2021). Developing a conceptual model for insider threat. *Journal of Management & Organization*, *27*, 911-929. https://doi.org/10.1017/jmo.2018.57

Wilder, D. U. M. (2017). The psychology of espionage. *Studies in Intelligence, 61*(2), 19-36.

Williams, A. D., Abbott, S. N., Shoman, N., & Charlton, W. S. (2021). Results from invoking Artificial Neural Networks to measure insider threat detection & mitigation. *Digital Threats: Research & Practice, 3*(1), Article 3. https://doi.org/10.1145/3457909

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2021). Cognitive and behavioral radicalization: A systematic review of the putative risk and protective factors. *Campbell Systematic Reviews, 17*(3), e1174. https://doi.org/10.1002/cl2.1174

Yammarino, F. J., & Dansereau, F. (2002). *The Many Faces of Multi-Level Issues. Research in Multi-Level Issues, Vol. 1*. Elsevier Science: Oxford.

Yang, J., & Diefendorff, J. M. (2009). The relations of daily counterproductive workplace behavior with emotions, situational antecedents, and personality moderators: A diary study in Hong Kong. *Personnel Psychology, 62*(2), 259–295. https://doi.org/10.1111/j.1744-6570.2009.01138.x

Zhao, L., Lam, L. W., Zhu, J. N. Y., & Zhao, S. (2022). Doing it purposely? Mediation of moral disengagement in the Relationship between illegitimate tasks and counterproductive work behavior. *Journal of Business Ethics, 179*(3), 733–747. https://doi.org/10.1007/s10551-021-04848-7

Zhou, Z. E., Meier, L. L., & Spector, P. E. (2014). The role of personality and job stressors in predicting counterproductive work behavior: A three-way interaction. *International Journal of Selection and Assessment, 22*(3), 286–296. https://doi.org/10.1111/ijsa.12077

Zimmer, E., Burkert, C., & Federrath, H. (2021). Insiders dissected: New foundations and a systematisation of the research on insiders. *Digital Threats: Research & Practice*, 3(1), Article 2. https://doi.org/10.1145/3473674

Appendix A: Definitions

Example Definitions of "Insider"

Alawneh and Abbadi (2011) - users should have authorized credentials enabling them to access organization sensitive content to be considered as insiders'; An insider is an internal or external user who "uses credentials", obtained by either authorized or unau- thorized means, to access sensitive corporate information that results in harm to the organization. Such a misuse could be either accidental or deliberate.

BaMuang et al. (2018) - In general terms, an insider has been defined as "someone who is entrusted with authorized access, who instead of fulfilling assigned responsibilities, manipulates access to a system to exploit it."

Bulling et al. (2008) - An insider is someone within an organization or with access to critical aspects of the organization. An insider can be an employee, contractor, consultant, or any person who has a relationship with or is in a position of trust within the organization. The insider may be someone acting alone or in collusion with others.

Elmrabit et al. (2015) - "Is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure", simply as: an individual who has authorized access to an IT system.

Bishop et al. (2005) - defined an insider in terms of how s/he is trusted with respect to the assets of an organization: "an insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure"

Althebyan & Panda (2007) - an insider is "an individual who has the knowledge of the organization's IS structure for which he/she has authorized access and who knows the underlying network topologies of the organization's IS."

Greitzer and Frincke (2010) - define the insider as "an individual currently or at one time authorized to access an organization's IS, data, or network."

Predd et al. (2008) - an insider "is some- one with legitimate access to an organization's computers and networks. an insider might also be represented by an external entity such as contractor, ex-employee, or business partner."

Example Definitions of "Insider Threat"

Bishop et al. (2005) – "… a trusted entity that is given the power to violate one or more rules in a given security policy … the insider threat occurs when a trusted entity abuses that power"

Bishop & Gates (2008) – "a trusted entity that is given the power to violate one or more rules in a given security policy... the insider threat occurs when a trusted entity abuses that power."

Bailey et al. (2018) – "the cyberrisk posed to an organization due to the behavior of its employees, rather than other kinds of insider threat, such as harassment, workplace violence, or misconduct. For these purposes, contractors and vendors are also considered employees; many of the largest cases in recent memory have trusted third parties at their center."

BaMaung et al. (2017) – "insider threat develops from someone who has access to privileged resources and exploits those privileges, but is furthered by those members of an organization who also have knowledge of internal information systems, may be involved in decision making and who are in positions of authority over critical operations."

The National Insider Threat Task Force (NITTF) – "a threat posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any U.S. government resource."

Bulling et al. (2008) – "A threat posed by an insider to an organization can be intentional or the result of negligence on the part of the insider. Threats refer to behaviors and related actions that pose a risk to the organization, as opposed to the presentation of threatening language alone. Threats that are particularly concerning include sabotage, espionage, theft, politically motivated violence, terrorist acts, or general disruption to organizational infrastructure or security. Such threats may originate from inside or outside an organization. The actions that make up threats like sabotage, espionage, terrorist acts, or insider threats include a range of individual behaviors that are often referred to as behaviors of concern."

Elmrabit et al. (2015) – "(a) Any malicious activities that cause damage to an organisation's IT and network infrastructure, applications, or services - (b) On the part of an employee (current or former), contractor, subcontractor, supplier, or trusted business partner - (c) Who has or has had authorised access to the organisation's IT assets - (d) And poses a significant negative impact on the information security elements (confidentiality, integrity, and availability) of the organization."

Elmrabit et al. (2020) – "malicious or unintentional activities on the part of an employee (current or former), contractor or trusted business partner, who has, or has had, authorised access to the organisation's IT assets, that cause damage to the organisation's assets and/or has a significant negative impact on the information security elements of the organisation (i.e. confidentiality, integrity and availability of information)."

Greitzer et al. (2016) – "a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and who intentionally (or unintentionally) exceeds or misuses that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems."

Pfleeger et al. (2010) – "an insider's action that puts at risk an organization's data, processes, or resources in a disruptive or unwelcome way."

Greitzer & Frinke (2010) – "harmful acts that trusted insiders might carry out; for example, something that causes harm to an organization, or an unau- thorized act that benefits the individual."

Theoharidou et al. (2005) – "threats originating from people that have been given access rights to an IS and misuse their privileges, thus violating the IS security policy of the organization."

Cappelli et al. (2012) – "Is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.”

Bailey et al. (2018) – “Malicious insiders are those who purposefully seek to benefit themselves at the organization’s expense or to harm the organization directly. They might steal valuable data, commit fraud for financial gain, publicly expose sensitive information to attract attention, or sabotage IT systems in disgruntlement. Most organizations focus their attention on malicious insiders, using activity-monitoring software and small investigative teams.”

Appendix B: Integrated Insider Threat Models

Bedford & van der Laan (2021), p. 1196

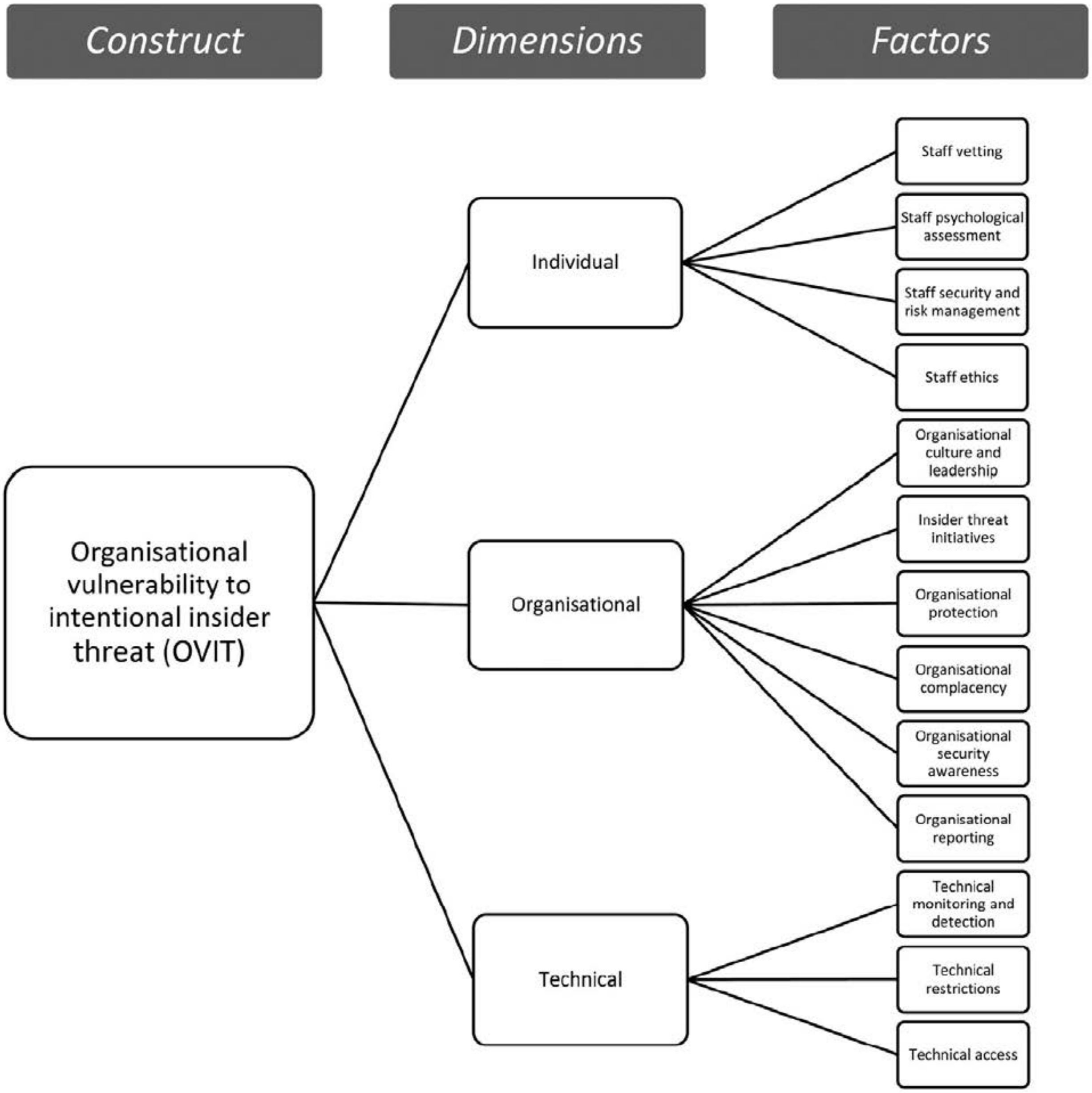

Construct
Dimensions
Factors
Organisational vulnerability to intentional insider threat (OVIT)
Individual
Organisational
Technical
Staff vetting
Staff psychological assessment
Staff security and risk management
Staff ethics
Organisational culture and leadership
Insider threat initiatives
Organisational protection
Organisational complacency
Organisational security awareness
Organisational reporting
Technical monitoring and detection
Technical restrictions
Technical access

Figure 8. The OVIT framework and factor structure of individual, organisational, and technical dimensions.

Whitty (2021), p. 924

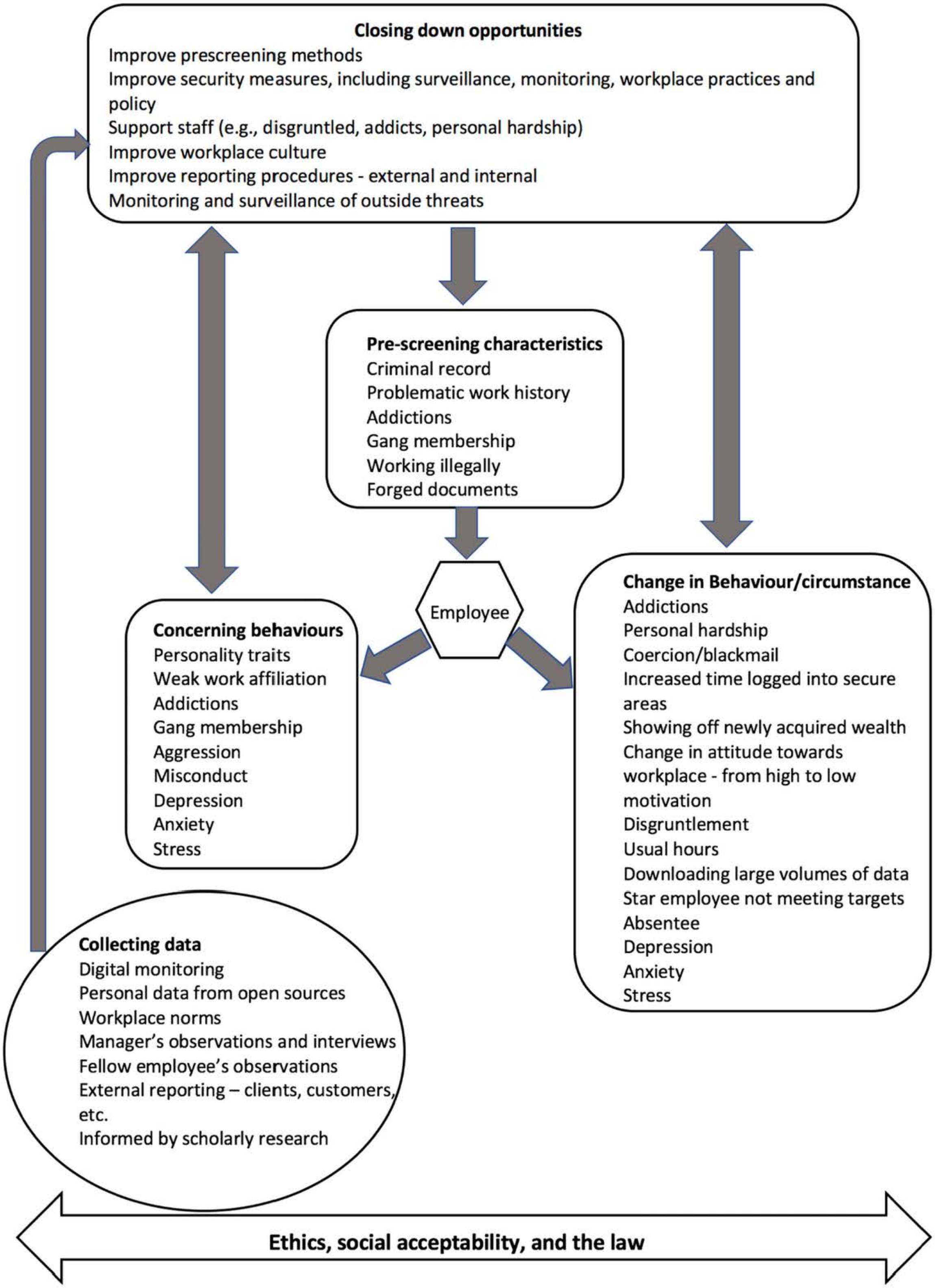

Closing down opportunities
Improve prescreening methods
Improve security measures, including surveillance, monitoring, workplace practices and policy
Support staff (e.g., disgruntled, addicts, personal hardship)
Improve workplace culture
Improve reporting procedures - external and internal
Monitoring and surveillance of outside threats
Pre-screening characteristics
Criminal record
Problematic work history
Addictions
Gang membership
Working illegally
Forged documents
Employee
Concerning behaviours
Personality traits
Weak work affiliation
Addictions
Gang membership
Aggression
Misconduct
Depression
Anxiety
Stress
Change in Behaviour/circumstance
Addictions
Personal hardship
Coercion/blackmail
Increased time logged into secure areas
Showing off newly acquired wealth
Change in attitude towards workplace - from high to low motivation
Disgruntlement
Usual hours
Downloading large volumes of data
Star employee not meeting targets
Absentee
Depression
Anxiety
Stress
Collecting data
Digital monitoring
Personal data from open sources
Workplace norms
Manager's observations and interviews
Fellow employee's observations
External reporting – clients, customers, etc.
Informed by scholarly research
Ethics, social acceptability, and the law

Figure 1. Prevention and detection of insider attacks

Elmrabit, Yang, Yan, & Zhou (2020), p. 5

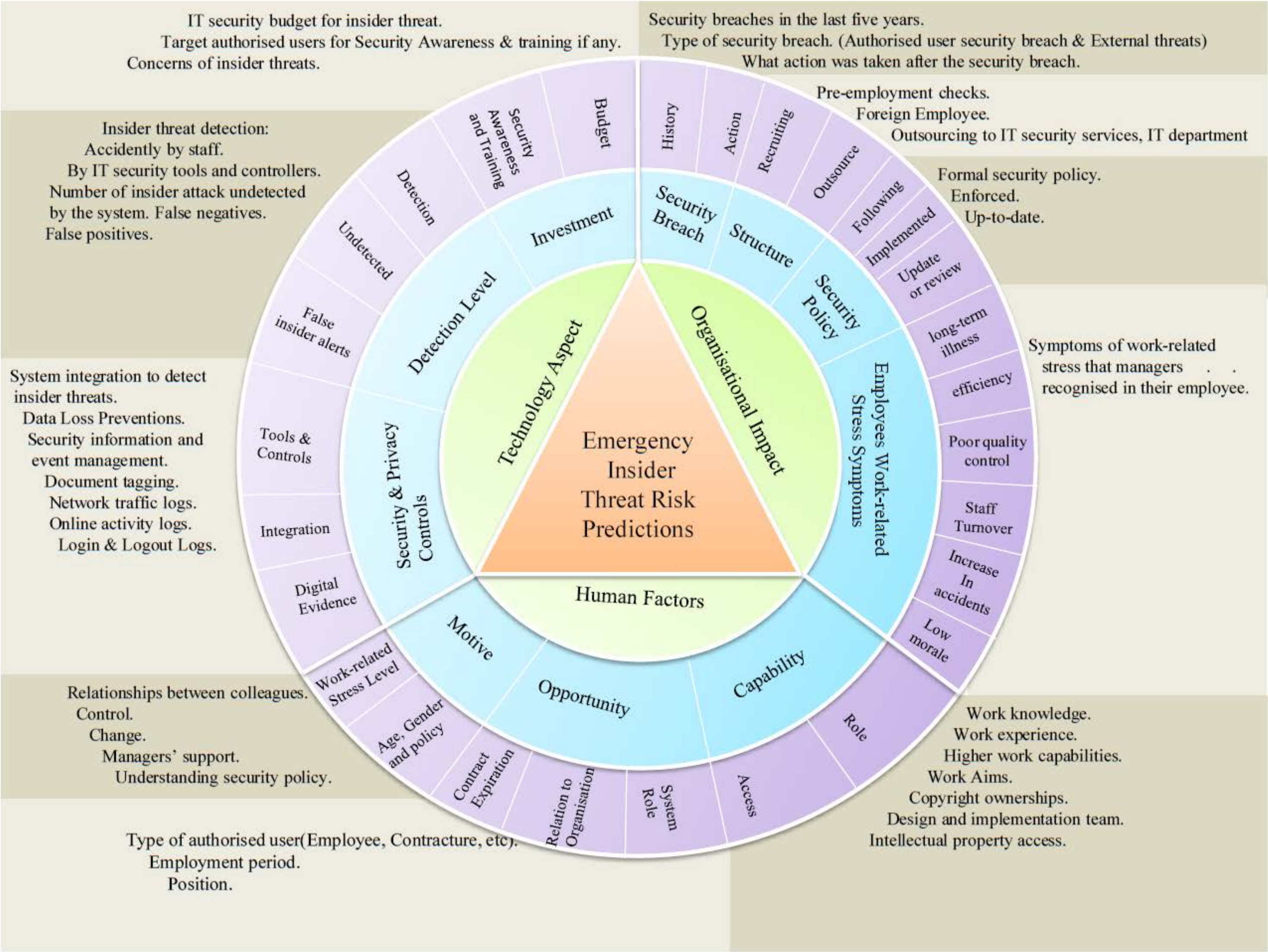

Emergency Insider Threat Risk Predictions
Technology Aspect
Organisational Impact
Human Factors
Investment
Detection Level
Security & Privacy Controls
Security Breach
Structure
Security Policy
Employees Work-related Stress Symptoms
Motive
Opportunity
Capability
Budget
Security Awareness and Training
Detection
Undetected
False insider alerts
Tools & Controls
Integration
Digital Evidence
Work-related Stress Level
Age, Gender and policy
Contract Expiration
Relation to Organisation
System Role
Access
Role
History
Action
Recruiting
Outsource
Following
Implemented
Update or review
long-term illness
efficiency
Poor quality control
Staff Turnover
Increase In accidents
Low morale
IT security budget for insider threat.
Target authorised users for Security Awareness & training if any.
Concerns of insider threats.
Security breaches in the last five years.
Type of security breach. (Authorised user security breach & External threats)
What action was taken after the security breach.
Pre-employment checks.
Foreign Employee.
Outsourcing to IT security services, IT department
Formal security policy.
Enforced.
Up-to-date.
Insider threat detection:
Accidently by staff.
By IT security tools and controllers.
Number of insider attack undetected by the system. False negatives.
False positives.
System integration to detect insider threats.
Data Loss Preventions.
Security information and event management.
Document tagging.
Network traffic logs.
Online activity logs.
Login & Logout Logs.
Symptoms of work-related stress that managers . . recognised in their employee.
Relationships between colleagues.
Control.
Change.
Managers' support.
Understanding security policy.
Type of authorised user(Employee, Contracture, etc).
Employment period.
Position.
Work knowledge.
Work experience.
Higher work capabilities.
Work Aims.
Copyright ownerships.
Design and implementation team.
Intellectual property access.

Figure 1: Framework for Insider Threat Risk Prediction