


Scholarship In Practice

# Seven (Science-Based) Commandments for Understanding and Countering Insider Threats

Eric L. Lang<sup>1</sup> <sup>a</sup>

<sup>1</sup> Office of People Analytics, Personnel and Security Research Center (PERSEREC)

Keywords: insider threat, human factors, continuous evaluation, mental health, organizational culture, insider threat program, insider threat policies, counter-insider threat, Psychology, Behavioral Science, Human Resources

---

## Counter-Insider Threat Research and Practice

Vol. 1, Issue 1, 2022

---

Insider threats are a growing problem that undermine organizations and national security. Understanding and reduction of some types of insider threats has improved, but significant gaps, emerging risks, and untapped opportunities remain. The purpose of this article is to highlight the criticality of human factors and social science approaches to countering insider threats and to share seven useful sets of overarching insights, evidence, and recommendations gleaned from over 35 years of research. Although good policy and technological tools are necessary, they are not sufficient. Reliable technological safeguards are important, and software, hardware, and data science innovations should be vigorously pursued to help reduce insider threats. But because insider threats are instigated or facilitated by human behavior, technological developments must involve social scientists and subject matter experts. If enough individuals in an organization have sufficient knowledge, skill and, most important, personally-felt commitment to protect the safety, security, and well-being of their colleagues and organization, even limited insider threat policies will succeed. Without individuals' sincere commitments, the most extensive insider threat policies will fail.

### Introduction

Organizational problems are rising. Serious data breaches, thefts of intellectual property (IP), and network compromises resulting from malicious, negligent, externally coerced, and well-meaning rule breakers within organizations have increased dramatically (Ponemon Institute, 2020; VentureBeat, 2022) Without effective management, such insider threats can undermine mission execution, employee safety, productivity, morale, financial stability, network functioning, asset integrity, public welfare, and local and global trust.

“Insider threat” is an umbrella term covering the potential for “any person who has or had authorized access to, or knowledge of, an organization’s assets and resources, to use their authorized access, wittingly or unwittingly, to bring harm to the organization’s mission, resources, personnel, facilities, information, equipment, networks, or systems” (U.S. Cybersecurity & Infrastructure Security Agency, n.d.). No sector, including government agencies, industry, acad-

eme, and nonprofit groups, has proven to be immune. The growing volume, interconnectedness, and access to sensitive electronic information increases the speed and scope of compromises. Insiders are especially dangerous due to their privileged knowledge and access regarding their organization’s valuable assets and security safeguards. Because insiders sometimes collaborate with, or unwittingly succumb to influences by, malicious outsiders—such as business competitors, foreign intelligence services, greedy or angry ex-employees, extremists, and disruptive high-tech vandals—aggregate insider risks threaten national security.

Understanding and reduction of some types of insider threats has improved, but significant gaps, emerging risks, and untapped opportunities remain. The purpose of this article is to highlight the criticality of human factors and social science approaches to countering insider threats (in contrast to purely technological approaches) and to share seven useful sets of overarching insights and recommendations gleaned from studies at PERSEREC (Lang, 2022)

---

<sup>a</sup> Director, Defense Personnel and Security Research Center (PERSEREC), Office of People Analytics (OPA), U.S. Department of Defense. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the DoD, OPA, or PERSEREC. The author greatly appreciated insights and suggestions from CITRAP anonymous reviewers, CITRAP editorial staff, several government stakeholders and, especially, PERSEREC government and contractor colleagues whose research, creativity, and dedication—throughout PERSEREC’s 36 year history—were inspirations for this article. Correspondence concerning this article should be sent to Eric.L.Lang6.civ@mail.mil or PERSEREC@mail.mil.

and from other researchers over the past 35 years.<sup>1</sup> Because each set of insights offers a broad prescriptive standpoint on countering insider threats, they are summarized as seven science-based “commandments” to guide understanding, application, and further research. Given that their primary value derives from being evidence-based, testable, and open to debate, I hope and expect they will be subject to research-grounded revision. Considering such prescriptions first requires an understanding of the types and seriousness of the problems they are designed to address.

### Scope of the Problem

Insider threats cover an extremely diverse set of problems. Although historic attacks by insider spies such as Robert Hanssen and terrorists such as Nidal Hasan are typically the most damaging—resulting in multiple deaths and major compromises of classified national security plans—they are rare events and, by far, the most infrequent types of harm caused by insiders. As described by the Institute for Critical Infrastructure Technology (2017), insider threats generally occur in the following forms, in decreasing frequency (this author’s editorial extensions are shown in *italics*):

1. “Careless, *[overloaded,]* or uninformed insiders who unintentionally violate security requirements and policies due to a lack of cybersecurity awareness *[, motivation, inadequate staffing, impaired ability to follow required procedures, or ineffective]* training.
2. Negligent insiders who intentionally evade security measures out of convenience, neglect, or misguided attempts to increase productivity *[or satisfy urgent supervisor demands]*.
3. Malicious insiders who intentionally evade security measures in attempts to profit financially, gain revenge, or *[expose perceived malfeasance, often]* based on a misguided sense of idealism.” (Institute for Critical Infrastructure Technology, 2017)

A fourth (and least frequent) form of insider threat may also be noted:

4. *Coerced insiders who unintentionally fall victim to external malicious persons using blackmail, intimidation, and related pressure tactics.*

Insider threat incidents also result from negligence by an organization’s IT staff (see box, above), such as delayed deployment of critical system patches (Ponemon Institute, 2022; Robb, 2022), especially if the staff are stressed by

poor organizational culture (see 6<sup>th</sup> Commandment) and related burnout (Sherman, 2022).

With respect to IT use by employees, although social media platforms such as LinkedIn and Facebook offer excellent resources that support professional productivity, they are also increasingly being exploited by malicious individuals and State actors who surveil, entice, and entrap insiders, particularly those with knowledge pertaining to security, intelligence, technology, and sensitive IP (Homeland Security Today, 2022). Consequently, increased use of social media platforms that mix professional and personal aspirations, particularly those accessed through personal versus company-managed networks, will increase the vulnerability of insiders to malicious social engineering efforts.

Specifically, the shift among many sectors from office-based work to remote work, which increased steeply in 2020 because of Covid-19 and is likely to continue at high levels post-Covid, substantially exacerbated insider threat problems (Ponemon Institute, 2020; VentureBeat, 2022). For example

- 62% of employees say they do not follow security protocols as closely as they do when they are in the office.
- Employees are 85% more likely today to leak files than they were pre-COVID.
- 75% of insider threat criminal prosecutions involved remote workers.

Managing the variety and increasing frequency of insider threats will require concerted and strategic collaborations among governments, industry, academe, and individuals. Basic and applied science, creativity, political will, and individual awareness and responsible behavior will be key. The effectiveness of this approach will directly affect the well-being and viability of individuals, organizations, and nations.

### Seven Science-Based Commandments for Countering Insider Threats

Although the U.S. government has mostly separate Insider Threat and Personnel Security policies and oversight offices, other western governments and non-governmental organizations meld them because the two areas overlap substantially in concerns for identifying and reducing risky behavior. This article takes a broad approach to insider threats, addressing areas of mutual interest.<sup>2</sup> Similarly, the Threat Lab—founded by PERSEREC and co-sponsored by the National Counterintelligence and Security Center

1 This article and the recommendations it articulates reflect the author’s Social and Behavioral Science perspective based on research and experiences working at PERSEREC from 2000-2022. Although PERSEREC’s work focuses primarily on government organizations, policies, and insiders, the insights, recommendations, and tools have increasingly been of interest to non-governmental organizations and stakeholders, especially since PERSEREC founded the Threat Lab in 2018.

2 Because personnel issues have far reaching influences, the seven Commandments relate to areas well beyond Insider Threat and Personnel Security, such as Information Security, Cybersecurity, Physical Security, HR, and Organizational Development. Similarly, some insights and recommendations will pertain more to government agencies (such as the 3<sup>rd</sup> Commandment), whereas others will be relevant to all organizations.

## National Security Concern: Types, Trends, and Magnitude of Insider Threats

Insider threats cover an extremely diverse set of problems, including

- **Government/Corporate Espionage**  
e.g., insider provides classified information to an unauthorized group or steals IP for personal gain
- **Extremism/Terrorism/Violence**  
e.g., radicalized insider turns violent
- **Vandalism/Disruption**  
e.g., vengeful insider harms the organization’s computer system
- **Reliability Problems and Gross Negligence (Including Well-Meaning Rule Breakers)**  
e.g., insider with alcohol or substance abuse problems, psychological problems, or gross incompetence fails to protect sensitive information/systems
- **Self-Harm and Suicide**  
e.g., insider plans suicide. There have been debates on whether it is appropriate and helpful to include self-harm; however, some policies include it because it can result in personnel injury or death.

Characterizing Malicious Insider Incidents	Characterizing Unintentional/Negligent Insider Incidents
<ul style="list-style-type: none"> <li>• 62% involved employees trying to establish a second income stream from their employer’s sensitive data</li> <li>• 29% stole information as they exited employment for future financial gain</li> <li>• 9% were saboteurs (Thundium, 2017)</li> </ul>	<ul style="list-style-type: none"> <li>• Poor endpoint security</li> <li>• Unsecured cloud systems</li> <li>• Undeployed critical patches</li> <li>• Backup failures or corruption</li> <li>• Internet of Things device insecurity</li> <li>• Inadequate Bring Your Own Device policies</li> <li>• Unsecured Wi-Fi networks (Robb, 2022)</li> </ul>

### Insider Threat Incidents Increasing

- 44% increase in insider threat incidents across all types of organizations (2020-2022; Ponemon Institute, 2022)
  - 56% of reported incidents were due to negligence.
  - 26% of incidents were related to criminal insider behavior.
  - 18% of incidents were related to user credential theft (credential approximately doubled in frequency between 2018 and 2022).
  - The average annual cost to remediate a negligence incident was \$6.6 million.
- 72% increase in actionable insider threat incidents in the industry sector in 2021 compared to 2020 (VentureBeat, 2022)
  - 56% of organizations had an insider data theft resulting from employees leaving or joining the company.

(NCSC) and DoD’s Counter-Insider Threat Program—builds on extant research and best practices to accelerate critical understanding, useful improvements, broad application, and collaboration among government policy makers, operations managers, scientists, security and HR professionals, and organizational leaders (Lang, 2022). To that end, we propose seven science-based prescriptions in the form of commandments.

### 1st Commandment: Human factors are paramount. Thou shalt not worship technology above personal and social dynamics solutions.

For understanding and mitigating insider threats, technological factors are important, but human factors are

more important. Across all forms of insider incidents that have occurred, the majority of prevention, detection, and mitigation failures have been due to human behaviors (e.g., delays in reporting concerning behaviors of coworkers and social engineering manipulations) rather than technological weakness (e.g., insufficient automated network monitoring).

One example comes from PERSEREC’s research program that explores trends, over decades, of espionage (Herbig, 2017)—principally Americans convicted of spying against the United States—and sensitive “resource exfiltration,” (Jaros et al., 2019) a broader category that includes insider violations such as unauthorized removal and hoarding of classified documents.<sup>3</sup> The most recent exfiltration study found that 73% of insiders did not use technological means

<sup>3</sup> The number of U.S. laws used to prosecute espionage-related crimes has increased over time. Of special note, (1) the 1917 Espionage Act does not require that violated information be classified; (2) espionage need not involve a foreign government—several cases covered in the PERSEREC report involved leaks to American citizens and/or the media; and (3) additional relevant laws include the 1938 Agents of Foreign Governments Act, export laws enacted in the 1970s, and the 1996 Economic Espionage Act.

to accomplish their exfiltration. The most common method used was to conceal resources in a container of some kind (e.g., a briefcase or bag) or in clothing (e.g., a pocket or under a hat). Eleven perpetrators did not physically exfiltrate documents or devices but, instead, memorized and later transferred sensitive information (Jaros et al., 2019). In these cases, security technology in place was insufficient.

In the business sector, a key finding from the Human Factors Report (Proofpoint, 2022) indicates “Remote work, supply chains, commercial clouds offer threat actors social engineering opportunities to trick people into doing their bidding...In the vast majority of cases, human factors matter more than the technical specifics of an attack, the researchers maintain. Cybercriminals are looking for relationships that can be leveraged, trust that can be abused, and access that can be exploited” (Mello, 2022)

The difficulty is that social science solutions are often more complicated, ambiguous, and time-consuming to define, develop, implement, and maintain than technological solutions. Yet human factors continue to be key in the biggest insider threat gaps and the greatest opportunities for progress. Addressing such challenges can be compounded by a sense of urgency and frustration over worsening insider threat trends or by experiencing a dire insider breach. Too frequently this results in a rush to show senior stakeholders and partners that the organization will “do something” (e.g., upgrade User Activity Monitoring software), which can lead to a false sense of security that the organization is sufficiently protected. Better protected?—yes. Sufficiently protected?—no.

To be clear, reliable technological safeguards are important, and software, hardware, and data science innovations should be vigorously pursued to help reduce insider threats. But because insider threats are instigated or facilitated by human behavior, technological contributions by software programmers must be done in concert with input by social scientists and subject matter experts (such as personnel experts) in the domain targeted for application. For example, insider threat technology and algorithms developed primarily through “brute empiricism” and atheoretical predictive modeling, regardless of the quantity of data points analyzed and the sophistication of machine learning methods applied, often result in products that are fast, pervasive, and powerful yet incomplete, biased, and ineffective. The security literature is rife with examples of expensive, useless, and unethical technology tools that were not developed and field-tested with sufficient social science input (Dyson et al., 2021; New York Times, 2022; O’Neil, 2016)

The good news is that

1. There are many relevant and effective C-InT approaches and applications grounded in years of social science theory, development, and field testing to

draw upon (e.g., Shaw & Sellers, 2015; Theis et al., 2019).

2. Every year there are more promising integrations of advanced technology (e.g., machine learning combinations of “User and Entity Behavior Analytics” and “Security Information and Event Management”) with principles of psychology and behavioral science. (See, for example, presentations at the annual Workshop on Research for Insider Threats.<sup>4</sup>)
3. To help address lingering problems where social science approaches continue to be underutilized, misunderstood, or misapplied, an increasing number of government and nongovernment organizations, and, as of 2022, the CITRAP journal, are raising awareness of social science advances and best practices for understanding, preventing, and mitigating insider threats. (e.g., NCSC, 2021)

## **2<sup>nd</sup> Commandment: Employees are an organization’s greatest strength, especially for identifying insider threats. Thou shalt improve supervisor and coworker reporting.**

Assessments of most insider threat incidents, especially those that involved malicious intent, indicate that someone in the organization was aware of risky, anomalous, or other behavioral indicators of concern and either failed to report their concern or the reported concern was mishandled by others. Given that most organizations have some form of “See Something, Say Something” workplace reporting policy, the question arises, why is there weakness in reporting systems that cover indicators of concern? The answer lies in understanding the four parts of a reporting system. Specifically, how indicators of concern should be identified, reported, assessed, and followed up.

**Indicator Identification.** Although artificial intelligence systems are increasingly capable of distinguishing meaningful indicators of human speech, written text, facial expressions, body movements, and activity patterns, such systems still are neither located pervasively enough nor as capable as modern humans have become after 300,000 years of communal living to correctly integrate and interpret the myriad subtle, variegated, and ambiguous “signals” that emanate from individuals each second. Consequently, the perceptions and responsible actions of conscientious staff who are aware of the typical, aberrant, and norm-appropriate behaviors, emotions, and patterns of individuals in their work environment—often with experiences of them outside of work situations—will continue to represent the greatest potential for pervasive, reliable, and timely information on possible indicators of insider threat.

**Indicator Reporting.** If humans are the best indicator detectors and organizations have insider threat reporting policies, why is there a reporting problem? Research has

---

4 Workshop on Research for Insider Threats (WRIT): <https://writ.compute.dtu.dk/>

shown that individuals are reticent to report on coworkers (e.g., Warble, 2018). Several causes include:

- Socialization and cultural norms, e.g., “don’t be a snitch”
- Expectations of peer loyalty, e.g., “code of silence”
- Concerns about the outcome, e.g., “I don’t want coworker to lose his job”
- Fear of retaliation, e.g., “that person, their boss or other parts of the organization, will get back at me”
- Diffusion of responsibility, e.g., “Many others are aware; I’m sure somebody will report it”

Additionally, reporting processes are not always well understood, including

- What to report? Sometimes less is more (Wood et al., 2005)
- How to report (to whom)?
- What will happen after a report is made?

Consequently, the overall approach to improving reporting (e.g., Nelson et al., 2019) is to

1. Establish a clearly defined reporting process.
2. Make the outcome of the process transparent.
3. Increase felt responsibility and mutual responsibility.
4. Make the process non-punitive.
5. Eliminate risks associated with disclosure.
6. Train and test employee understanding and ability.
7. Emphasize the positive aspects of reporting such as preventing a larger problem or safety risk to others as well as facilitating help or support for a struggling coworker.

Because frontline supervisors have responsibilities for their direct reports and often are in a unique position to observe indicators of concern, PERSEREC is developing customizable software, tentatively titled “Supervisor Guide to Concerning Conduct” that will include

- Guide to Concerning Behavior—How to identify employee behaviors of concern
- Employee and Organizational Wellness—How to deal with barriers to taking action
- Supervisor Actions—How to address concerning employee behaviors.

**Indicator Assessment and Follow-up.** Most of the seven steps listed above are inextricably connected to what employees and supervisors are told, how they are trained, and, more important, what they perceive regarding how their organization assesses and follows up on indicator reports. These factors are addressed in Commandments 3 through 7.

**3<sup>rd</sup> Commandment: Initial personnel screening is critical but not sufficient. Thou shalt focus on improving comprehensive, fair, and effective continuous vetting.**

Why is initial personnel screening critical? It is important to vet applicants thoroughly to reduce the likelihood that the new insider (1) has, or will succumb to, malicious

intentions, or (2) has, or is developing, thought patterns, or other dispositional issues that would substantially undermine their reliability for protecting sensitive resources and personnel. For eligibility to access classified information (commonly referred to as a Security Clearance), this goal was codified in a U.S. Executive Order (EO) titled “Access to Classified Information,” which states

...eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. (EO 12968, 1995)

In the decades since this law was established, social scientists, government leaders, technologists, and many others have struggled to define and operationalize concepts like “trustworthiness” and “character” into vetting practices that are valid, reliable, effective, efficient, and fair. As of 2022, U.S. security clearance vetting policies—including initial and continuous vetting—are codified in nine Security Executive Agent Directives (SEADs 1-9) issued by ODNI. The mandate for insider threat programs to protect classified information was established by EO 13587 (2011), *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. More general government vetting policies covering unclassified situations (e.g., suitability for government employment) are issued primarily by the Office of Personnel Management.

Why should continuous vetting get greater attention? Clear evidence comes from PERSEREC research on unclassified espionage incidents and trends that cover hundreds of Americans convicted of espionage-related offenses since World War II (Herbig, 2017). Two findings are particularly pertinent.

First, during the over 70 years covered by this research, although persons who held Top Secret clearances were required to undergo periodic reinvestigations (PRs) every 5 years, the continuous evaluation during the 5-year intervals was weak, relying primarily on self-reports of significant life changes and personal problems. Some convicted spies commented that they viewed the PR policies and operations as a 5-year opportunity to misbehave, in some cases intensifying their espionage with the intent to exit from government employment prior to their next PR.

Second, and more important, of more than 200 convicted spies, all but one (Ana Montes) appear to have entered their government employment without malicious insider threat intentions. This implies that they passed their initial vetting correctly and then later developed problems (e.g., financial needs, severe grievances, or divided loyalties) that resulted in espionage. Although, the U.S. Government has made substantial progress enhancing Continuous Vetting, industry and other non-governmental organizations, on av-

erage, do not have fair and cost-effective continuous vetting systems in place.

It is beyond the scope of this paper to cover details on how to conduct continuous vetting at national and organizational levels. However, as a general principle, the goal is to integrate multiple appropriate, high-quality data inputs that cover sources and adjudication guidelines pertinent to the organization's insider threat concerns. Examples include certain arrest, travel, financial, and social media records that have been determined to contain accurate and relevant information and that do not violate the rights of the individual being vetted. Overall, for any new data input being considered for initial or continuous evaluation, three questions should first be addressed:

1. *Investigation*<sup>5</sup>—Are the prospective data relevant, reasonably free of errors, and ethical to use?
2. *Authentication*—How will operators confirm that person identities in the data are accurate? and
3. *Adjudication*<sup>6</sup>—How will operators ensure that data-based vetting decisions align with legal, relevant, and effective adjudication procedures?

**4<sup>th</sup> Commandment: Indicator lists, algorithmic flags, and predictive models are essential but limited. Thou shalt ensure effectiveness through follow-up procedures that are timely, integrative, transparent, and humane.**

Simple solutions are super. Unfortunately, when faced with complicated, high-risk, ambiguous problems, individuals often find too much comfort in simple lists and automated tools that have neatly repeatable processes. For countering insider threats, standardized indicator lists and automated risk assessment models can lull well-intentioned professionals into an overly optimistic sense that the hardest part of the problem has been addressed. It has not. Well-developed<sup>7</sup> indicator lists and risk prediction models are essential, but they are only a first step. The more important step is follow-up. In other words who, using what procedures, will address indicators of potential concern that surface? To understand the challenge, it is necessary to appreciate the limitations of indicator lists and predictive models.

The primary limiting quality of most indicators, especially those based on a single observation, derives from the challenge of drawing reliable inferences from a brief occurrence, i.e., many human behaviors and their causal origins are ambiguous. Here are two examples using items common to government-issued and other reasonable insider threat indicator lists (e.g., CISA, 2020): (1) signs of alcohol abuse, drug misuse or illegal drug use, and (2) attempts to access files or facilities not clearly within the employee's work responsibilities. Item #1 would require reporting an employee displaying classic signs of being drunk such as slurred speech, unsteadiness, and confusion. However, these are also signs displayed by an individual with diabetes experiencing hypoglycemia (low blood sugar levels). Behaviors in item #2 may derive from an employee's malicious attempt to steal important files or from a conscientious employee's eagerness to learn about additional parts of their organization to better serve the organization's interests.

Building predictive models is also hampered by the fact that the most devastating incidents are rare. Using espionage as an example, even though there is information on over 200 convicted spies since WWII, there have been over 20 million individuals with security clearances during the same timeframe.<sup>8</sup> It is statistically not viable to create a valid and reliable predictive model on complex events that occur at a population rate of 1/100,000.

Predictive models typically analyze numerous sources of risk-related information. How well could a model predict an incident that is more prevalent than convicted government spies such as insider theft of unclassified sensitive information? The challenge to accurate prediction is that some incidents evolve through slow, deliberative planning, while others happen quickly during a perceived window of opportunity. Perpetrators' motivations have varied widely, including greed, ideology, vengeance, egotism, extremism, and divided loyalties. Overall, the range and dynamic interactions among individuals' antecedent behaviors, emotions, cognitions, motivations, and contextual influences is so great within each of the five categories of malicious and unintentional insider threats (outlined at the beginning of this article) that no model has yet demonstrated it can produce valid, reliable, and reasonably precise timeline predictions of a specific individual attempting an incident of concern (e.g., see New York Times, 2020).

---

5 PERSEREC conducted the proof-of-concept research and prototype development that laid the foundation for modern continuous vetting (Herbig et al., 2013).

6 For U.S. Security Clearances, adjudication guidelines were initially developed by PERSEREC (Carney & Marshall-Mies, 2000), along with an explanatory adjudication reference (Heuer & Gregory, 2014), and then later revised by ODNI as SEAD-4, *National Security Adjudicative Guidelines*.

7 A well-developed indicator list, predictive model, or other insider threat identification method is one created through relevant and ethical procedures that identifies an acceptably large proportion of individuals who pose a real threat while minimizing false alarms, that is, falsely identifying individuals as threats.

8 "20 million" is a conservative estimate based on several data-based assumptions from open source government reports (e.g., ODNI, 2010): (1) since 2010 there has been an annual average of four million individuals with security clearances, (2) an annual turnover rate of approximately 10%, e.g., replacements due to cleared individuals retiring or moving into uncleared positions, (3) a burgeoning of clearance holders after 9/11, 2001 and (4) a slow increase of 10% annually of cleared individuals between 1945-2001.

Nevertheless, well-developed predictive models are important and useful for two reasons. First, they can assist leaders and insider threat professionals to better understand which individual dispositions (e.g., personality and mental health conditions) and contextual factors (e.g., toxic workplace climates, and helpful HR interventions) can interact over time to exacerbate or ameliorate insider threat potential and improve general predictions. Greitzer's research on Insider Threat Predictive Analytics (e.g., Greitzer, 2022) and the Critical Pathway model (Shaw & Sellers, 2015) are helpful in this regard. Second—and this also pertains to well-developed indicator lists—predictive models can greatly reduce the number of employees the organization needs to follow up, which decreases investigative and HR costs as well as unnecessary intrusions on employees and other insiders who pose no threat.

Regarding the indicator list examples #1 and #2, both employees should be reported to a relevant authority immediately and without presumption or prejudice. The same is true for insiders flagged by well-developed predictive models. In all cases, the key to effective insider threat management depends on the speed and quality of follow-up.

Speedy follow-up analysis is important so that indicators determined to be (1) imminent threats can receive timely attention (e.g., communicated to a security, law enforcement, or counterintelligence office); (2) non-imminent, unintentional, acute personal struggles, or patterns of coping problems can receive prompt non-punitive support or intervention as necessary (e.g., from a supervisor, HR, or an occupational health representative; and (3) non-threats can have their indicator status removed quickly (e.g., to reduce the potential for stigma by organizational staff with access to insider threat operations data). In combination, these three factors will support insider threat management that is both effective and humane.

Most important is the composition of the insider threat team that assesses indicators and manages follow-up actions. Because, as described, the most frequent type of insider threats are “careless or uninformed insiders who unintentionally violate security requirements and policies due to a lack of motivation, inadequate staffing, impaired ability to follow required procedures, or ineffective cybersecurity training,” the insider threat team should include specialists in HR, security, clinical psychology (or behavioral analytics), and, preferably, an insider threat specialist.

Ideally, the insider threat assessment and management team should have a mandate, authorization, and capability to (1) integrate information quickly from multiple sources (e.g., initial screening, continuous vetting, training outcomes, HR and annual performance records, and supervisor and coworker reports) and (2) order interviews, psychological evaluations or other assessments of individuals as necessary. Finally, the policies and operating procedures of the team should be transparent to all employees, which can help in building trust and personal commitment throughout the organization (for more detail, see the 6<sup>th</sup> Commandment).

### **5<sup>th</sup> Commandment: Most mental health conditions are neither dangerous nor insider threats. Thou shalt honor and educate the whole organization about mental health, promote help-seeking, and reduce mental health stigma.**

The general public and too many senior leaders, supervisors, and security professionals continue to falsely believe that mental health problems are closely linked with a high risk to commit violence and compromise sensitive information. These beliefs undermine productive and fair security and insider threat mitigation practices and exacerbate harmful mental health stigma. Such practices and stigma can incentivize insiders to not seek necessary treatment—raising the likelihood that their condition will worsen and affect their performance—or to lie on vetting forms about treatment they have received (lying on security forms can be grounds for job punishment or termination).

Unfortunately, the challenge is made more difficult by limited access to mental health services and stigma. For example

- One in five U.S. adults experience mental illness each year, but less than half of them receive treatment. (Center for Behavioral Health Statistics and Quality, 2021)
- The average delay between onset of mental illness symptoms and treatment is 11 years. (Wang et al., 2004)
- Half of workers are concerned about discussing mental health issues in the workplace; a third worry about consequences if they seek help. (American Psychiatric Association, 2019)

Some mental health conditions are common. For example, about 25% of all adults will experience clinical levels of anxiety or depression at some time in their lives. Many individuals are able to cope with these conditions without professional services. Clinical treatment for these and most other conditions is often effective, allowing individuals to perform their jobs reliably.

The American Psychological Association recently summarized facts about the association between mental illness and violence based on multiple, high-quality, national studies:

1. *"The vast majority of violent acts are not due to mental illness, and most people with mental illness are not violent.*
2. *When people with mental illness do commit violence, it is often due to contextual or background factors such as a history of childhood physical abuse, living in poor and/or dangerous neighborhoods, or using substances.*
3. *Factors that predict violence for all people—antisocial behavior, substance use, and anger issues, for example—also predict violence in individuals with mental illness.*
4. *Committing a violent act is rare, under 3% among individuals with serious mental illness, which is only slightly higher than the percentage for all individuals in the general population" (DeAngelis, 2021).*

Mental health stigma affects many individuals who seek or have a Security Clearance, even though evidence consistently shows that only 5 of every 100,000 (i.e., 0.005%) individuals will have their security clearance denied or revoked solely because of a psychological issue (Defense Counterintelligence and Security Agency, 2022).

While the most common mental health conditions pose virtually no substantial security risk, several Psychological conditions and behavior patterns do represent Insider Threat concerns in that they can undermine an individual's judgment, stability, reliability, or trustworthiness. For any individual, the behaviors of concern may or may not have been caused by a formal clinical disorder—and a clinical diagnosis is not necessary for there to be a concern. For obtaining and keeping a Security Clearance, examples of concern include patterns of “irresponsible, violent, self-harm, suicidal, paranoid, manipulative, impulsive, chronic lying, deceitful, exploitative, or bizarre behaviors” (SEAD, 2017).

Specific, formal, mental health disorders of concern (e.g., because—without effective treatment—they can compromise reliable behavior and security-conscious judgment) include “psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder, or antisocial personality disorder” (Office of Personnel Management, 2016; Shedler & Lang, 2015). Certain rare psychological syndromes are also of concern, especially clinical levels and combinations of psychopathy, malignant narcissism, and borderline personality organization, which have been shown to predict maladaptive functioning, employment trouble, and forensic risk (Lang, 2011; Shechter & Lang, 2011).

As described in the 4<sup>th</sup> Commandment, fast, high-quality follow-up is key once evidence of a concerning behavior pattern or mental health condition has surfaced. Even if a concerning mental health condition is confirmed, the risk can often be mitigated by evidence that it has been (or will be) addressed by appropriate mental health treatment.

Organizational leaders should not assume that, because they have issued supportive mental health policies and messages, all staff understand and agree. In industry, for example, two recent national surveys found that, although over 70% of employers reported that they were adequately supporting their employees' mental health needs, only 27% of their employees agreed (Coe et al., 2021). Consequently, an organization's mental-health-related policies—especially those pertaining to insider threat—must be clear and appropriate and combined with effective efforts to

- educate the entire workforce about (1) mental health facts, support options, observations that should be reported, and (2) the organization's policies and approach to addressing Mental health issues,
- reduce mental health stigma,
- promote open and safe dialog,
- support seeking treatment,

- bolster self-help and resilience skills, and
- assist all staff on how to recognize a coworker who needs help and how to follow-up appropriately.

In addition to reducing mental health risks associated with insider threat, such efforts will support overall organizational morale and trust (the focus of the Commandment 6).

**6<sup>th</sup> Commandment: Leadership and organizational culture at every level are key. Thou shalt help senior leaders, managers, and especially frontline supervisors to develop healthy, psychologically safe, and inspiring organizational cultures.**

For countering insider threat, as with most other aspects of organizational performance, clear policies, commitment, and resource support from senior leadership are the necessary first steps to healthy and productive functioning. Unfortunately, these steps alone do not ensure good organizational culture and outcomes. Organization culture is generally understood to be a shared set of employees' perceptions and assumptions that affect their expectations and behaviors. Organizational culture differentially affects each individual's subjective psychological contract—essentially, the quid pro quo between an individual and the organization for which they work (Bankins et al., 2020). Consequently, this unspoken psychological contract is the individual-level result of organizational culture and the most important determinant of what a worker is willing to do (e.g., level of effort, loyalty, and adherence to rules) in exchange for what the individual expects the organization to provide (e.g., meaningful tasks, fair treatment, a reasonable level of personal control, acceptable pay, and a humane, preferably supportive, work climate).

When workers perceive that their organization has negatively shifted some aspect of the organizational culture, (e.g., their supervisor's management style has eroded from benign to toxic), they see the quid pro quo of their psychological contract as broken. This often results in employees negatively shifting their part of the equation such as reducing their effort, engaging in counterproductive workplace behaviors, leaving the organization, or, in extreme cases, engaging in serious insider threat activities. This was a major theme of the Federal Government's 2021 National Insider Threat Awareness Month “NITAM” (NCSC, 2021).

Most organizations still pay too little attention to their organizational culture, preferring, instead, to issue formal policies, blanket messaging, and additional requirements. Good policies provide a necessary foundation, but they are not sufficient. When it comes to day-to-day organizational functioning, mission outcomes, and employee engagement: organizational culture eats policy for breakfast.<sup>9</sup>

---

<sup>9</sup> This relates to an expression attributed to management guru Peter Drucker in 2006 that “Culture eats strategy for breakfast.”

Research consistently confirms the harm of negative organizational culture. A study that relates to the 5<sup>th</sup> Commandment on mental health showed that in organizations characterized by a lack of consideration, knowledge, and empathy regarding mental health issues, employees were 300% more likely than employees in other organizations to develop significant depressive symptoms (Zadow et al., 2021). Another common consequence is employee burnout (Sherman, 2022). With respect to insider threat, research has shown that burned out employees are substantially less likely to adhere to security requirements (59% for burned out employees vs. 80% for others). Similarly, burned out employees are much more likely to download and use software without their organizations' permission (48% vs. 30%; 1Password, 2021).

In contrast, respectful, supportive and positive workplace cultures help to build a workforce infused with trust. In addition to reducing contextual influences that breed insider threats, trust yields substantial organization-wide benefits: "Compared with people at low-trust companies, people at high-trust companies report: 74% less stress, 106% more energy at work, 50% higher productivity, 13% fewer sick days, 76% more engagement, 29% more satisfaction with their lives, 40% less burnout." (Zak, 2017). Similar research showed that employees who felt more psychologically safe were significantly more likely (than employees who felt less psychologically safe) to report unethical behaviors they observed in their workplace (Ferrere et al., 2022).

Organizational culture starts at the top. Specifically, with the extent to which senior and mid-level leaders are perceived by their workforce as being good (or poor) models of integrity, honesty, compassion, rule-adherence, diligent work ethic, diversity and inclusion, and other values that they say are important for all workers to embrace and exhibit. For example, a recent study concluded "...our research has revealed another key finding that seems to hold true for virtually every organization we have worked with: *the vast majority of experiences of exclusion are attributed to people, not policies.*" Respondents cited "leadership" (59%) and "direct supervisors" (37%) as the primary causes of their experiences of exclusion (Zang, 2021).

Considering all aspects of organizational culture, the biggest influences come from frontline supervisors. All employees have a direct supervisor. A supervisor typically has more frequent contact (than do other managers) with their own direct reports and usually influences their work assignments, feedback, rewards, promotion potential, level of work stress, and other important quality-of-work-life factors (Holm et al., 2021).

Unfortunately, employees are often promoted into a team-leader or supervisory role primarily because of their technical skills or accomplishments as an individual contributor. Such promotions produce inept managers (Benson et al., 2019). Fifty years of Industrial-Organizational Psychology and Management research has shown that supervisory and leadership roles require a whole set of additional interpersonal "people skills" (e.g., Argyris, 1962; Katz, 1974). Such skills include active listening, mentoring, ex-

pressing honest appreciation, trust building, interpersonal problem solving, fair and effective disciplining, encouragement, clear and productive communication, team building, helpful empathy, and creating a psychologically safe work climate (e.g., Edmondson, 2018), all of which foster a healthy, trusting, and productive organizational culture. Training for new supervisors is typically superficial with respect to these critical skills with greater focus, instead, on administrative functions such as reviewing employees' time cards, approving leave requests, and procedures to execute a performance improvement plan.

The difficulty is that improving organizational culture and supervisors' people skills require in-person time from Supervisors and competent trainers and, consequently, is often perceived as being too expensive (compared to sending management memos and offering "canned" automated tutorials). Yet there is no alternative. An organization's productivity, well-being, and ability to counter insider threats are at stake. In the long run, so is national security. The 7<sup>th</sup> Commandment offers a science-based recommendation.

**7<sup>th</sup> Commandment: Meaningful metrics and behavior-based training are essential. Thou shalt forsake quick and dirty education and assessment methods (even if it is all that is required to show compliance).**

For continuous improvement of any individual, corporate, or enterprise-wide function, it is imperative to define process and outcome metrics carefully so that they relate closely to desired goals and are amenable to valid empirical input assessed in sufficient quantities and frequencies. Such metrics support useful insights and action. Where human performance is a goal, or human factors are key to achieving a higher-order goal, education and training are typically necessary. To better understand and counter insider threats, the evidence and logic supporting the seven Commandments indicate the path to improvement is paved with human factors issues. Because there is adequate coverage in journals and textbooks of common measurement foci including the basic forms of reliability and validity, and the challenge of proving a negative, this section will, instead, highlight three areas that require greater attention and investment to better counter insider threats. The areas involve improving the (1) measurement of key contextual influences, (2) "ecological validity" of measurement methods, and (3) relevance and effectiveness of education and training methods.

**Improving the Measurement of Key Contextual Influences.** The majority of research on insider threat produced by scientists and practitioners—especially in the "Western World," e.g., the U.S., UK, Australia, Canada, and New Zealand (the "Five Eyes" allies)—focuses overwhelmingly on individuals' background history and dispositions, e.g., personality, mental health, cognitive patterns, motivations, and emotional states. This focus likely comes from western historical roots that view individuals' dispositions as the principal (often exclusive) causal force determining their

behaviors and, consequently, why individuals should be held completely accountable for their actions. It partly accounts for why we are so uncomfortable to hear of good people doing bad things. We discount the possibility that contextual factors played a major role and could have had a comparable influence on any good person (like ourselves). It is more comfortable to believe the bad actor was always bad or made bad personal choices. This philosophy is reflected in employment screening systems, security clearance vetting, legal systems, and insider threat programs. Individuals' backgrounds and dispositions are important causative factors, but there is much more.

Decades of industrial/organizational and social psychology research show the majority of human behavior, as well as the myriad of dispositions that underlie it, are constantly being shaped (since birth) by different levels of contextual factors, such as the influence of family members, friends, office colleagues, work culture, religious communities, and societal norms. Interactions over time between dispositional and contextual factors can be difficult to parse, but one conclusion is clear: Contextual factors greatly influence the development of individuals' good and bad behaviors. Two well-researched social psychology books on the dynamics of contextual influences to negatively shape the behaviors of otherwise normal individuals are worth studying: Kruglanski and Bélanger's (2019) *The Three Pillars of Radicalization: Needs, Narratives, and Networks*, and Zimbardo's (2008) *The Lucifer Effect: Understanding How Good People Turn Evil*. In industrial/organizational psychology, hundreds of research studies have elucidated workplace contextual influences, how they can spread, and how they can be addressed (e.g., Bergland, 2021).

With respect to insider threat, contextual factors are critical, under-researched, and poorly measured. Organizational culture is amenable to improvements and tools for promoting such change are available (e.g., Wilson et al., 2022). Future research in this area needs to better identify key contextual factors that directly and indirectly shape the development of insider threats. Exacerbating and ameliorative factors should both be explored including psychological safety, tolerance for rule-breaking, incivility, harassment, discrimination, aggression, noxious competitiveness, organizational citizenship, toxic vs supportive supervision styles, stressful vs humane office climates, and insecurity-laden vs trust-building organizational cultures. Once these factors are identified, the challenge is how to improve the "ecological validity" of how they are measured.

**Improving the Ecological Validity of Measurement Methods.** Whether research is performed in a lab, a work setting, or some other field environment, "ecological validity" refers to how relevant, accurate, and useful the research measurements are for populations in real-world settings. Improving ecological validity can be difficult. Research done in a lab allows for better isolation and control over factors of interest, but often at the cost that lab-based insights and interventions are too artificial and do not effectively transfer as needed in less-controlled real-world settings.

In addition to performing more insider threat related research and intervention trials in real-world settings, such research needs to complement survey and self-report measurement methods with more ecologically valid "unobtrusive measures" (i.e., measures that are less likely to involve the awareness and opinions of the individuals being studied). For example, in addition to surveying workers on the level of hostile communications they perceive, unobtrusive measures could be assessed, such as automated anonymized analyses of aggressive semantics in emails, and anonymized audio analyses of loud and aggressive discussion tones in office areas. Subjective perceptions are important. Objective unobtrusive data are important, but typically not collected. Employing and comparing subjective and objective data enhances research-based insights, understanding of outcome metrics that need to be tracked, and the development of effective education and training interventions (e.g., Reader et al., 2020).

**Improving the Relevance and Effectiveness of Education and Training Methods.** In many areas, static documents and prepackaged automated tutorials (if developed well) are effective for gaining certain kinds of factual knowledge. When real-world situations require knowledge coupled with behavioral skills, training needs are different. You cannot learn to ride a bike by watching an online slide tutorial. The same is true for learning how best to behaviorally respond to stressful and ambiguous insider threat situations, as well as for developing more helpful and effective social interaction skills to lead or supervise a team. For developing effective behavioral skills, especially for application in complex, dynamic, and stressful situations—as is often the case for countering insider threats—you must get on the bike. Ideally, a skilled instructor is present to help (Parsons et al., 2012).

Instructional documents and automated tutorials are typically time-efficient, low cost, and standardized. For many important insider threat and organizational culture related behavioral skills, they are often ineffective. For example, tutorials may change participant's attitudes. But that may not carry over into desired behavioral outcomes. Here is an example:

Organizations often assume that if they understand and impact insiders' security culture and attitudes, they will necessarily improve related behaviours, but we should avoid assuming that an affected attitude will always (or even mostly) carry forward into a desired behaviour change, e.g., in a university-based research study, among individuals who said they would report sexual harassment, only 20% actually did (in the study virtual organizational setup), even when reporting the sexual harassment incident only required them to click on a link. Studies like this highlight the need to define and implement effective training and measure critical behavioral outcomes, in addition to changes in knowledge, attitudes, and culture. (Goodwin et al., 2020)

One best practice for dynamic behavior-based training is to employ interactive didactic discussions of insider cases, where the instructor pauses throughout each case timeline to ask participants, "at this point, who knows what?; What

could or should be done?; What are the risks and ethics of different options?; What would you do, and why?” “Red Teaming” as well as exercises of contacting employees with realistic test emails and calls, e.g., to assess and improve behavioral capabilities against Phishing and Vishing, can be useful (KnowBe4, 2022). Another best practice for effective preparation for insider threat situations that may involve a personal encounter in the workplace, such as preventing a person “tailgating” through a secure entrance, or responding to an encounter involving potential aggression, theft, or concerning mental health issues, is guided role playing in realistic scenarios. Role playing and simulations, in addition to building skills and confidence, influences (and is influenced by), psychological safety (Purdy et al., 2022).

A tool useful for leader-facilitated insider threat training—developed by PERSEREC’s Threat Lab and its partners at the Office of the Undersecretary for Defense for Intelligence and Security and NCSC—is called “In Retrospect.” It is an insider threat video series that features interviews with people who have first-hand experience with a real insider threat case. These videos are designed to be used by any organization interested in facilitating training and discussion around hard questions and dilemmas related to insider threat detection, mitigation, and prevention.

Unsurprisingly, behavior-based training is also key for developing supervisor “people skills” highlighted in the 6<sup>th</sup> Commandment for building healthy, psychologically safe, and inspiring organizational cultures that reduce insider threats. In addition to promoting positive and productive working environments that ameliorate insider threats, supervisors are in an ideal position to employ their people skills as an important bridge between line staff and upper management (i.e., for conducting small-group meetings where insider threat policies, programs, and organizational goals, along with staff perceptions, concerns, and questions can be discussed safely). When done well, such discussions build knowledge, trust, and help individual staff members develop a personal commitment to protecting the safety, security, and well-being of their colleagues and organization. Because personal commitment motivates behavior better than officiously mandated compliance, such commitment should also be measured and valued as an organizational outcome of interest.

Metrics based on individuals’ performance in realistic (i.e., ecologically valid) hands-on training will usually yield more reliable indicators (than simple knowledge and confidence tests needed to pass self-administered slideshows) of actual effective readiness. This is a vital skill-based out-

come quality that organizations need to increase to counter insider threats. Test takers’ feelings of confidence in performing a complex skill after watching an online tutorial are often unrelated to their actual competence in a real situation (Jordan et al., 2022). Unfortunately, cost is often the enemy of quality. Behavior-based training incurs instructor time and more participant time than prepackaged slide shows. This is where organizational leadership is crucial. Hard decisions must be made to better balance cost-effectiveness considerations, and not to succumb to low-cost options that meet superficial “check-the-box” training compliance requirements.

When individuals and organizations are rewarded for meeting superficial requirements, their goals and programs will fail. Management expert Steven Kerr (1975) described it best as “the folly of expecting A while rewarding B.”

## Conclusions

Insider threats are a growing problem that undermine organizations and national security. The seven Commandments cover science-based insights and options for success. Although good policy and technological tools are necessary, they are not sufficient. For countering insider threats, the most important gaps and opportunities require greater attention to human factors issues and field-tested applications grounded in basic and applied social sciences. Extant Social and Behavioral Science insights, tools, and best practices can be drawn upon now to counter insider threats and improve workplace security, management, training and, especially, organizational culture. Although several guides and tools are provided throughout this paper, for many applications the specifics of “who” and “how” to effect improvements will depend on the organizational component structure, leadership style, extant policies, and available internal resources. Despite those circumstantial differences, the seven Commandments highlight an overarching theme: Insider threats are done by individuals and most can be prevented by individuals. If enough individuals in an organization have sufficient knowledge, skill and, most important, personally felt commitment to protect the safety, security, and well-being of their colleagues and organization, even limited insider threat policies will succeed. Without individuals’ sincere commitments, the most extensive insider threat policies will fail.

Submitted: June 03, 2022 PDT. Accepted: July 21, 2022 PDT.

Published: August 02, 2022 PDT.



This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CCBY-NC-ND-4.0). View this license’s legal deed at <https://creativecommons.org/licenses/by-nc-nd/4.0> and legal code at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode> for more information.

## References

- 1Password. (2021). *The burnout breach: How employee burnout is emerging as the next frontier in cybersecurity*. <https://1password.com/resources/2021-state-of-secure-access-report/>
- American Psychiatric Association. (2019). *About Half of Workers Are Concerned about Discussing Mental Health Issues in the Workplace; A Third Worry about Consequences if They Seek Help*. <https://www.psychiatry.org/newsroom/news-releases/about-half-of-workers-are-concerned-about-discussing-mental-health-issues-in-the-workplace-a-third-worry-about-consequences-if-they-seek-help>
- Argyris, C. (1962). *Interpersonal competence and organizational effectiveness*. Dorsey Press.
- Bankins, S., Griep, Y., & Hansen, S. D. (2020). Charting directions for a new research era: Addressing gaps and advancing scholarship in the study of psychological contracts. *European Journal of Work and Organizational Psychology*, 29(2), 159–163. <https://doi.org/10.1080/1359432x.2020.1737219>
- Benson, A., Li, D., & Shue, K. (2019). Promotions and the Peter Principle. *The Quarterly Journal of Economics*, 134(4), 2085–2134. <https://doi.org/10.1093/qje/qjz022>
- Bergland, C. (2021, June 25). Rudeness: How workplace incivility spirals out of control. *Psychology Today*. <https://www.psychologytoday.com/us/blog/the-athletes-way/202106/rudeness-how-workplace-incivility-spirals-out-control>
- Carney, R. M., & Marshall-Mies, J. C. (2000). *Adjudicative guidelines and investigative standards in the Defense Department (TR 00-02)*. Defense Personnel Security Research.
- Center for Behavioral Health Statistics and Quality. (2021). *2020 National Survey on Drug Use and Health (NSDUH): Key Substance Use and Mental Health Indicators in the United States*. Substance Abuse and Mental Health Services Administration. <https://www.samhsa.gov/data/>
- Coe, E., Cordina, J., Enomoto, K., Mandel, A., & Stueland, J. (2021, April 21). *National surveys reveal disconnect between employees and employers around mental health need*. <https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/national-surveys-reveal-disconnect-between-employees-and-employers-around-mental-health-need>
- Cybersecurity and Infrastructure Security Agency. (2020). *Insider Threat Mitigation Guide*. [https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide\\_Final\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf)
- DeAngelis, T. (2021). Mental health and violence: Debunking myths, addressing realities. *APA Monitor*, 52(3), 31–36. <https://www.apa.org/education-career/ce/mental-illness-violence.pdf>
- Defense Counterintelligence and Security Agency. (2022). *Mental health and security clearances*. [https://www.cdse.edu/Portals/124/Documents/webinars/DCSA-FactSheet\\_Mental-Health.pdf](https://www.cdse.edu/Portals/124/Documents/webinars/DCSA-FactSheet_Mental-Health.pdf)
- Dyson, F., Fukuyama, F., Forster, E., Welin, S., Joy, B., Heilbroner, R., Pinch, T., Bijker, W., Hughes, T., Latour, B., Lessig, L., Hopkins, P., Winner, L., Ritzer, G., Dyer, R., Weber, R., Sarewitz, D., Wetmore, J., McCray, W., ... Bess, M. (2021). 23 Franken-Algorithms: The Deadly Consequences of Unpredictable Code. In *Technology and Society: Building Our Sociotechnical Future* (pp. 357–366). MIT Press.
- Edmondson, A. (2018). *The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth*. John Wiley & Sons.
- Exec. Order 12968. (1995, August 7). *Access to classified information*. [https://www.dni.gov/files/NCSC/documents/Regulations/EO\\_12968.pdf](https://www.dni.gov/files/NCSC/documents/Regulations/EO_12968.pdf)
- Ferrere, A., Rider, C., Renerte, B., & Edmondson, A. C. (2022). Fostering Ethical Conduct Through Psychological Safety,” in “Working Values: How Purpose, Morals, and Meaning Build Stronger Organizations. *MIT Sloan Management Review*, 19–23.
- Goodwin, R., Graham, J., & Diekmann, K. A. (2020). Good intentions aren’t good enough: Moral courage in opposing sexual harassment. *Journal of Experimental Social Psychology*, 86, 103894. <https://doi.org/10.1016/j.jesp.2019.103894>
- Greitzer, F. (2022, March 23). *Adventures in insider threat predictive analytics*. The Human Centric AI Seminars. [https://research.csiro.au/distributed-systems-security/wp-content/uploads/sites/113/2022/03/Greitzer\\_CSIRO-Data61-Seminar-FINAL\\_23March2022.pdf](https://research.csiro.au/distributed-systems-security/wp-content/uploads/sites/113/2022/03/Greitzer_CSIRO-Data61-Seminar-FINAL_23March2022.pdf)
- Herbig, K. L. (2017). *The expanding spectrum of espionage by Americans, 1947 – 2015 (TR-17-10)*. Defense Personnel and Security Research Center/Office of People Analytics.
- Herbig, K. L., Zimmerman, R. A., & Chandler, C. J. (2013). *The evolution of the Automated Continuous Evaluation System (ACES) for personnel security (TR 13-06)*. Defense Personnel and Security Research Center.
- Heuer, R. J., & Gregory, E. R. (2014). *Adjudicative desk reference: Assisting security clearance adjudicators, investigators, and security managers in implementing the U.S. Government personnel security program*. [https://www.dhra.mil/Portals/52/Documents/perserec/ADR\\_Version\\_4.pdf](https://www.dhra.mil/Portals/52/Documents/perserec/ADR_Version_4.pdf)
- Holm, K., Torkelson, E., & Bäckström, M. (2021). Longitudinal Outcomes of Witnessed Workplace Incivility: A Three-Wave Full Panel Study Exploring Mediators and Moderators. *Occupational Health Science*, 5(1–2), 189–216. <https://doi.org/10.1007/s41542-021-00083-8>

- Homeland Security Today. (2022, May 17). *U.K. launches new app to counter malicious approaches online*. <https://www.hstoday.us/subject-matter-areas/cybersecurity/u-k-launches-new-app-to-counter-malicious-approaches-online/>
- Institute for Critical Infrastructure Technology. (2017, February 23). *The insider threat epidemic begins*. <http://icitech.org/event/icit-monthly-briefing-insider-threat/>
- Jaros, S. L., Rhyner, K. J., McGrath, S. M., & Gregory, E. R. (2019). *The Resource Exfiltration Project: Findings from DoD cases, 1985-2017 (PERSEREC-TR-19-02, OPA-2019-021)*. Defense Personnel and Security Research Center/Office of People Analytics.
- Jordan, K., Zajac, R., Bernstein, D., Joshi, C., & Garry, M. (2022). Trivially informative semantic context inflates people's confidence they can perform a highly complex skill. *Royal Society Open Science*, 9(3), 211977. <https://doi.org/10.1098/rsos.211977>
- Katz, R. (1974). Skills of an Effective Administrator. *Harvard Business Review*.
- Kerr, S. (1975). On the folly of expecting A while rewarding B. *Academy of Management Journal*, 18, 769–783.
- KnowBe4. (2022, July 19). *Phishing by Industry Benchmarking Report, 2022 Edition*. <https://info.knowbe4.com/phishing-by-industry-benchmarking-report>
- Kruglanski, A., & Bélanger, J. (2019). The three pillars of radicalization: Needs, narratives, and networks. *Oxford Scholarship Online*. <https://doi.org/10.1093/oso/9780190851125.001.0001/oso-9780190851125-chapter-1>
- Lang, E. L. (2011, May 25). *Improved Assessment of Personality Disorders that are Security Risks* [Conference presentation]. Annual meeting of the International Applied Military Psychology Symposium, Vienna, Austria.
- Lang, E. L. (2022). The Security Net, Safety Net, and Stakeholder Net for Countering Insider Threat. *Counter-Insider Threat Research and Practice*, 1(1).
- Mello, J. P. (2022, June 13). *Threat actors becoming more creative exploiting the human factor*. <https://www.csoonline.com/article/3663478/threat-actors-becoming-more-creative-exploiting-the-human-factor.html>
- NCSC. (2021, August 31). *NCSC and Federal Partners Kick Off "National Insider Threat Awareness Month"*. <https://www.dni.gov/index.php/ncsc-newsroom/item/2238-ncsc-and-federal-partners-kick-off-national-insider-threat-awareness-month>
- Nelson, L. C., Beneda, J. G., McGrath, S. M., & Youpa, D. G. (2019). *Enhancing supervisor reporting of behaviors of concern* [OPA Report No. 2019-033, PERSEREC-TR-19-0]. Defense Personnel and Security Research Center/Office of People Analytics.
- New York Times. (2022, May 17). *Your bosses could have a file on you, and they may misinterpret it*. <https://www.nytimes.com/2022/05/17/science/insider-threat-private-companies.html>
- Office of Personnel Management. (2016, November). *Standard Form 86: Questionnaire for National Security Positions*. [https://www.opm.gov/forms/pdf\\_fill/sf86.pdf](https://www.opm.gov/forms/pdf_fill/sf86.pdf)
- Parsons, M. B., Rollyson, J. H., & Reid, D. H. (2012). Evidence-based staff training: a guide for practitioners. *Behavior Analysis in Practice*, 5(2), 2–11. <https://doi.org/10.1007/bf03391819>
- Ponemon Institute. (2020, December). *Data exposure report 2021*. <https://www.code42.com/resources/reports/2021-data-exposure>
- Ponemon Institute. (2022). *2022 cost of insider threats global report*. <https://www.bloomberg.com/press-releases/2022-01-25/global-cybersecurity-study-insider-threats-cost-organizations-15-4-million-annually-up-34-percent-from-2020>
- Proofpoint. (2022). *The Human Factor Report 2022*. <https://www.proofpoint.com/us/resources/threat-reports/human-factor>
- Purdy, E., Borchert, L., El-Bitar, A., Isaacson, W., Bills, L., & Brazil, V. (2022). Taking simulation out of its "safe container"—exploring the bidirectional impacts of psychological safety and simulation in an emergency department. *Advances in Simulation*, 7(1). <https://doi.org/10.1186/s41077-022-00201-8>
- Reader, T. W., Gillespie, A., Hald, J., & Patterson, M. (2020). *Unobtrusive indicators of culture for organizations: A systematic review* [Manuscript].
- Robb, D. (2022, May 24). *Insider threats on the rise*. <https://www.cioinsight.com/leadership/insider-threats-on-the-rise/>
- SEAD-4: *National Security Adjudicative Guidelines*. (2017). <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf>
- Shaw, E., & Sellers, L. (2015). Application of the Critical-Path Method to evaluate insider risks. *Studies in Intelligence*, 59(2), 1–8. <https://nationalinsiderthreats.org/itrmresources/Application%20Of%20The%20Critical-Path%20Method%20To%20Evaluate%20Insider%20Risks-June%202015.pdf>
- Shechter, O. G., & Lang, E. L. (2011). *Identifying personality disorders that are security risks: Field test results (TR 11-05)*. Defense Personnel Security Research Center. <https://doi.org/10.21236/ada564011>
- Shedler, J., & Lang, E. L. (2015). A relevant risk approach to mental health inquiries in question 21 of the Questionnaire for National Security Positions (SF-86). In *TR 15-01*. Defense Personnel and Security Research Center/Defense Manpower Data Center. DTIC: ADA628339.
- Sherman, T. (2022, May 20). *How poor mental health can lead to bad security systems management*. <https://totalsecurityadvisor.blr.com/policies-training/how-poor-mental-health-can-lead-to-bad-security-systems-management/?Source=ITDA&effort=1&E2%80%A6>
- Theis, M. C., Trzeciak, R. F., Costa, D. L., Moore, A. P., Miller, S., Cassidy, T., & Claycomb, W. R. (2019). *Common sense guide to mitigating insider threats* (6th ed.). <https://resources.sei.cmu.edu/library/>

- U.S. Cybersecurity & Infrastructure Security Agency. (n.d.). *Defining insider threats*. <https://www.cisa.gov/defining-insider-threats>
- VentureBeat. (2022). *Insider risk intelligence and research report*. <https://venturebeat.com/2022/04/28/the-super-malicious-insider-and-the-rise-of-insider-threats/>
- Wang, P. S., Berglund, P. A., Olfson, M., & Kessler, R. C. (2004). Delays in initial treatment contact after first onset of a mental disorder. *Health Services Research*, 39(2), 393–416. <https://doi.org/10.1111/j.1475-6773.2004.00234.x>
- Warble. (2018). *2018 Workplace Experience Study, Volume 1: Why US Workers Remain Silent About Disruptive Behavior at Work*. <https://warble.work/why-us-workers-remain-silent-about-disruptive-behavior-at-work-2/#:~:text=39%25%20of%20respondents%20indicated%20that,a%20driver%20of%20employee%20silence>
- Wilson, G., Wolford, R., Beneda, J., Ellis, S. K., & Jaros, S. L. (2022). *Better ways to work together. A playbook for developing personal and organizational resilience* [OPA Report Number 2022-083, PERSEREC-PA-22-08]. Defense Personnel and Security Research Center/ Office of People Analytics.
- Wood, S., Crawford, K. S., & Lang, E. L. (2005). *Reporting of counterintelligence and security indicators by supervisors and coworkers (TR 05-06)*. Defense Personnel Security Research Center.
- Zadow, A. J., Dollard, M. F., Dormann, C., & Landsbergis, P. (2021). Predicting new major depression symptoms from long working hours, psychosocial safety climate and work engagement: A population-based cohort study. *BMJ Open*, 11(6), e044133. <https://doi.org/10.1136/bmjopen-2020-044133>
- Zak, P. J. (2017). The neuroscience of trust. *Harvard Business Review*, 95(1), 84–90.
- Zang, C. (2021). *People, not policies: The role of the individual in driving inclusion in the workplace*. <https://medium.com/aleria/people-not-policies-the-role-of-the-individual-in-driving-inclusion-in-the-workplace-6f80936f8171>
- Zimbardo, P. (2008). *The Lucifer effect: Understanding how good people turn evil*. Random House.