Munro, V. (2025). Insider threat typology – An analysis of motivational and behavioural attributes related to the violent extremist insider threat type. *Counter-Insider Threat Research and Practice*.

Original Research

Insider Threat Typology – an Analysis of Motivational and Behavioural Attributes Related to the Violent Extremist Insider Threat Type

Victor Munro[1,2a]

[1] Norman Paterson School of International Affairs (NPSIA), Carleton University, [2] Canadian Insider Risk Management Centre of Excellence (C-InRM CoE)

Keywords: Insider Threat, Extremism, Terrorism, Political Violence, Critical Infrastructure Protection, Risk Management, Security

Counter-Insider Threat Research and Practice

The linkage between violent extremism and insider threat has received heightened media coverage in the past few years and has highlighted the failures of organizational security programs to detect internal threats. While there has been a rapid increase in academic and industry studies on insider threat, there remains limited research on violent extremist insider threats, and there have been few empirical studies using real incident data to validate how it is distinct from other insider threats. This original research examines 122 cases of real extremist insider threat attacks using a logistic regression model that compares violent and non-violent observations. The results indicate that violent extremist insider threats are associated with grievances against the nation-state's policies and society in general as well as lower levels of income. The goal of this research is to inform organizational risk mitigation policy and programs—particularly in the critical infrastructure protection domain—about specific indicators related to violent extremist insider threat. Study limitations and avenues for future research are considered.

Detecting employees who seek to cause harm to their own organizations is a well-established problem for defensive counterintelligence (CI) programs (Lowenthal, 2002; Shulsky, 1991). Over the past decade, insider threat attacks—a domain of defensive CI—have increased in terms of negative impact to the assets of compromised organizations. As a result, there has been a corresponding increase in insider threat risk mitigation programs in the public and private domains (Kont et al., 2018). Insider risk programs seek to protect an organization's critical assets, employees, finances, sensitive data and intellectual property (IP), and reputation (Cybersecurity & Infrastructure Security Agency, 2020), from employees with privileged access who possess the capability to inflict harm (pre-conditions to be an "insider threat").

The insider threat characterized by violent extremism, defined as an act of violence that has been committed in the workplace as informed by an ideology (i.e., insider threat), is not well researched, despite significant negative consequences. These events impact even the largest organizations. Examples of harmful incidents impacting the United States Department of Defense (DoD) include the 2009 mass shooting at Fort Hood in Texas and the 2014 case of a U.S. national that joined the U.S. military for the express purpose of learning combat tactics that could be used to teach Islamic State (IS) fighters based in Syria (BaMaung et al., 2018). The latter example demonstrates that not all places of employment are necessarily the targets of insider threat attacks with different individual-level motivations; however, the presence of employees who conduct attacks outside the organization may nonetheless negatively impact an organization's reputation. Accordingly, the aim of the present study is to examine employee motivation and associated behavioral indicators, by examining "violent extrem-

a Mr. Munro is the Executive Director of the Canadian Insider Risk Management Centre of Excellence (CInRM CoE), based at the Norman Paterson School of International Affairs (NPSIA) at Carleton University (Ottawa, Canada). He is presently a Ph.D. candidate at NPSIA and employed as an insider risk management consultant. As part of his insider risk management work at Carleton University and the private sector, Mr. Munro is a sessional lecturer, provides mitigation services and training to Canadian public and private sectors, U.S. Fortune 500 companies, and speaks at industry forums.

He had held various positions within the Canadian security, intelligence, and defence communities for approximately two decades. During that time, he had participated in several partnership building initiatives at the international, federal, provincial, and municipal levels, in the public, private, and academic sectors. His academic and professional research interests and experiences include international affairs, WMD disarmament/arms control/non-proliferation, defence studies, trans-national conflict, national security policy, intelligence analysis, critical infrastructure protection, risk management, cyber security, criminal investigations, insider threat mitigation, terrorism studies, strategic foresight, and data exploitation.

ist"—as defined by the University of Maryland, National Consortium for the Study of Terrorism and Responses to Terrorism—insider threats and establishing how the motivational and behavioral attributes differ from other insider threats through a logistic regression analysis (University of Maryland, 2018).

To overcome gaps in organizational security programs and limit potential opportunities for attack, organizational risk mitigation policies must account for insider threats' motivational and behavioral attributes. There is general agreement in the present literature on the importance of understanding insider threat motivation and behavioral attribute data as a key element of effective risk mitigation programs. This data is used to inform detection capabilities to ensure that risk mitigation efforts using this data is undertaken through increased network and Internet-traffic monitoring to improve internal surveillance, enhance threat detection capabilities, and enable mitigative incident management and investigative responses to limit attack opportunities.

While statistical regression studies using real incidents of employee cyber-sabotage, fraud, and intellectual property (IP) theft, have identified statistically significant results concerning the associated motivational and behavioral attributes to these insider threats, there are other insider threats that are not accounted for in these studies—specifically violent extremist insider threats.

In this study, we hypothesize that the motivations and behaviors of employees who have become radicalized towards an extremist ideology vary from those of other insider threats, and present statistical evidence to display why violent extremist insider threats are different. A better quantification of the unique attributes of violent extremist insider threats would provide the basis for specialized monitoring programs and collection of data related to sentiment analysis for organizational risk mitigation purposes. The use of corporate internal networks and the Internet in the recruitment and radicalization of violent extremists has been well documented (National Institute of Justice, 2015). Research indicates that extremists' views are routinely inspired and reinforced through access to violent extremist forums, videos, and websites on the Internet, including via work computers (Centre for the Prevention of Radicalization Leading to Violence, 2016), with noted Islamist extremists Faisal Shahzad and Nidal Hassan being inspired to violence through postings on the Internet (Ornatowski & Pottathil, 2012).

Schoenherr and Thomson (2020) indicate that insider threats are a growing concern in security communities with a corresponding rapid increase in academic and industry studies on the topic, but BaMaung et al. (2018) indicate that there is a notable lack of research on the intersection between insider threat and violent extremism. The linkage between violent extremism and insider threat has received heightened media coverage in the past few years, and has highlighted the failure of organizational security programs in Western militaries and police forces to detect internal threats (Dearden, 2020; Pugliese, 2020; Sahinkaya, 2020). Unsurprisingly, security communities are focusing attention on this insider threat, acknowledging that while there are inherent challenges in terms of legal jurisdictional requirements for increased employee monitoring, individual free-speech and privacy rights, and maintaining a positive workplace culture, there are also real heightened risks to employees' physical safety, corporate assets, and reputation (Van Os et al., 2021).

A better understanding of the violent extremist insider threat will serve to inform public and private organizational insider threat risk mitigation policies and enhance organizational security programs in critical infrastructure sectors such as the government, information technology, military, energy, finance, and transportation, which have been subject to significant insider threat compromises over the past several decades (Maasberg et al., 2020). This study contributes to the existing body of literature in counterintelligence, terrorism, political violence, radicalization, insider threat and security studies, by examining what distinguishes violent extremist insider threats from other insider threats that have been described in academic literature to date.

In this paper we outline an underlying theoretical model and review key studies that have used real cases of insider threats to establish differences based on motivational and behavioral attributes. Anchored against these past studies, we present a series of hypotheses using attributes sourced from a U.S.-based dataset. We review the logistic regression method that was used in the data analysis and the results of the regression model. Finally, we conclude with a discussion of the findings and future avenues of research and policy recommendations.

Theory and Past Studies

At present, insider threat research is disproportionately published in computational science, engineering, and network security-related journals with modeling studies based on synthetic data that are not actual incidents of insider threat attacks. Critical evaluations are rare, and research methods in the insider threat literature are often based on intuition from subject matter experts, while computational models and empirical observations are based on synthetic or inaccessible "black" datasets. More research is required to reflect the varied motivations and behaviors presented by different insider threats (Schoenherr & Thomson, 2020).

Theories That Focus on the Role of Motivation

Insider threat theories are derived from outside of the existing CI literature and have become more sophisticated than simply just motivations linked to a strong attachment to a foreign identity, religious faith, or other ideological pre-disposition (Rudner, 2013), to focus on individual-level social-psychological root causes. Motivation is a causal mechanism within insider threat theories and is the focus of several insider threat studies. Different motivations have been the subject of focus depending on the insider threat being studied, including espionage, disgruntlement, revenge, financial, stress personal gain, organized criminal affiliations, (BaMaung et al., 2018; Maasberg et al., 2020;

Maasberg & Beebe, 2014; Whitty, 2021). Theories that have been applied from various academic disciplines to explain the motivational component includes deviance theory (sociology), routine activity theory (criminology), situational crime prevention (criminology), and rational choice theory (economics) (Mekonnen et al., 2015; Safa et al., 2018; Wang et al., 2015).

Theories That Focus on the Role of Behavior

Observable behavioral indicators, including substance addiction, poor and/or declining job performance, lack of trustworthiness, stress, and interpersonal conflicts in the workplace, have also been prominently featured as an area of focus within the literature across various insider threats (Ho et al., 2018; Maasberg et al., 2020; Maasberg & Beebe, 2014; Whitty, 2021). Theories and methods that have been applied from other academic disciplines to explain behavioral indicators and generate different insider threats include the "dark triad" of personality traits (including Machiavellianism, narcissism, and psychopathy) (Maasberg & Beebe, 2014), addiction theory (Maasberg & Beebe, 2014), signals detection theory (Mills et al., 2018), the bystander effect (to explain why colleagues of a potential insider threat may not report suspicious activity) (Bell et al., 2019), and inductive profiling (Maasberg et al., 2020).

Capability, Motivation, and Opportunity Theoretical Framework

The capability (to enable an attack), motive (to plan an attack), and opportunity (to initiate an attack) (CMO) theoretical framework was selected for this study as the most relevant for conceptualizing the causal motivations leading to specific behaviors and interactions with conditional opportunity mechanisms (based on insider threat risk mitigation policies and inherent organizational gaps) leading to potential insider threat attacks. While the dataset used in this study lacks information related to insider threat capability and opportunity, it does allow for an analysis of motivation and behavioral indicators—something that Maasberg et al. (2020) noted was missing in their past regression study that used another dataset. The CMO model originally developed by Schultz (2002) is foundational and frequently cited in insider threat studies. It postulates that insider threat attacks are caused by individual-level attributes and serves as the basis for insider threat risk mitigation policies and programs to develop preventative policy and program capabilities by accounting for attributes that can be further quantified through statistical regression, with indicator weightings calculated based on an aggregation of observed past insider threat attacks.

There have been a limited number of recent studies that have examined specific motivational and behavioral indicator data based on real incidents linked to specific insider threats. Maasberg et al. (2020) observed that current risk management practices require additional empirical validation of key risk indicators in the context of "cyber sabotage" towards the enhancement of insider threat mitigation programs. They conducted a logistic regression analysis on incidents of insider threat attacks and confirmed that specific attributes increased the likelihood of cyber-sabotage. The dataset that was used for the analysis was produced by the Carnegie Mellon (CM)-Computer Emergency Response Team (CERT)-Software Engineering Institute (SEI), and included coded attributes associated to individuals found criminally convicted of "malicious insider activity" in the U.S. since 1995. The study used the motivational aspect of the CMO theoretical framework; assuming that capability and opportunity existed in all incidents as they represented successful past compromises. The study focussed on motivational (defined as revenge, financial gain, and personal gain) and behavioral (defined as addiction, poor performance, and supervisor conflict) attributes as the independent variables, and examined how they associated with three different insider threat attack conditions including cyber-sabotage, fraud, and theft of IP as the dependent variables. This selection criteria resulted in a regression model that included 74 incidents, with a primary analysis that focused on cyber-sabotage as the main attack outcome. Addiction was found to be the most predictive indicator, while revenge, financial gain, addiction, and poor performance were statistically significant. In additional regression models involving fraud and theft of IP, the motivations of financial gain/supervisor conflict and financial gain/not seeking revenge were statistically more significant. The study was constrained due to missing motive and behavioral indicator data in several incidents found in the dataset which impacted sample size (Maasberg et al., 2020).

Mills et al. (2018) also focused on cyber sabotage; they reviewed potential insider threats against naval ship systems and used a regression-based model to validate that normal user patterns of behavior were different than malicious users based on unusual system login and device access frequencies (i.e., a greater focus on behavior based on the capability and opportunity components of the CMO theoretical model). The study utilized the CM-CERT-SEI dataset with statistically significant findings that legitimate users behave differently than malicious users (Mills et al., 2018).

Whitty (2021) undertook a qualitative, grounded theory analysis approach to identify which psychological, behavioral, and social variables (in cyber and physical contexts) were important in predicting insider attacks. This was done via semi-structured interviews of managers, co-workers, human resource employees, law enforcement, and security personnel associated to convicted insider threat actors within a year of an attack and resulted in a sample size of 99 case studies involving two to three individuals per study. The case studies consisted of 82% fraud attacks, with the remainder being reputational damage, theft (physical, identity and IP/data), money laundering, and illegal employment. The conceptual model that Whitty (2021) developed based on the results of the study, focused on organizational requirements to seek out "behavioral change indicators" and "close down opportunities" to prevent insider threat attacks. Whitty's (2021) findings indicate that although disgruntlement is often viewed as a requirement for insider threat, addiction and sudden changes in familial,

financial, or work performance indicators were found to be more relevant.

Limitations and Considerations for the Current Research

Sokolowski et al. (2016) were critical of insider threat research's focus on predicting attacks based on statistical models utilizing psychological and work environment variables. They found that focusing on past activity was problematic and did not necessarily account for the complexity and impact of changes that occur within an insider threat's organizational environment. Further, small sample sizes led to unsatisfactory indications towards predicting future insider threat attacks. This led Sokolowski et al. (2016) to develop a simulation that was tested against the CM-CERT-SEI dataset, of an insider threat becoming active within a dynamic organizational system. This was referred to as "agent-based modeling" to describe the complex adaptive behaviors of individuals within organizations.

While research on insider threat continues to gain prominence—Sokolowski's et al.'s (2016) criticisms on the direction of quantitative research studies aside—regression analysis undertaken by Maasberg et al. (2020) focussing on motivational and behavioral indicators is still limited. The absence of large sample studies makes it difficult to measure the external validity of findings. There is also limited generalizability when considering that the Maasberg et al. (2020) study focused on cyber-sabotage, IP theft, and fraud, but did not account for other insider threat physical attacks. Whitty's (2021) research by contrast, focused on IP theft and fraud, using axial coding based on the frequency of certain responses, but did not use regression analysis; however, it did produce similar results to Maasberg et al. (2020) in terms of motivation and behavioral indicators of importance.

Based on a review of ethics considerations, this research is relevant as it addresses a gap in the insider threat literature and will contribute to an existing body of knowledge concerning attributes of violent extremist insider attacks (Van Evera, 1997). When considering that terrorism has attracted widespread research interest since the September 11, 2001 (9/11) attacks in the U.S., the gap that this research addresses in present insider threat studies is notable when considering that the potential threat to organizations represented by violent extremist insider threats has not been explored with the use of regression analysis. Ba-Maung et al. (2018) notes that where these two subjects intersect, there is a requirement to better understand motivations and key behaviors. This imperative is due to violent extremist insider threat events leading to high human casualty consequences, including several notable Islamist extremist incidents since 2006 involving insider threats conducting information gathering and surveillance on behalf of listed entities, and attack plotting in the military and aviation sectors. In 2017, CM-CERT-SEI had expanded their definition of insider threat to include workplace violence (i.e., insider threats attacking another organization asset: its employees) (Cassidy, 2017). It was noted that the gathering of behavioral data is crucial to detecting workplace violence, "where the only manifestations of predicate indicators may be behavioral" (Cassidy et al., 2018). In a review of a limited sample of 26 cases of coworker-on-coworker incidents between 1986-2017, the underlying motivational attributes include revenge against the employer—manifested in these incidents as violent attacks against other employees, or opportunistically conducting violent attacks in the workplace, associated to indicators of financial stress, loss of significant other, conflicts with supervisors or co-workers, loss of employment, and/or substance abuse. Still, this does not fully address why violent attacks occur in organizations in the absence or presence of these motivational attributes—notably in cases of violent extremist insider threat attacks.

While there have been no notable studies of violent extremist insider threats using regression analysis, we reviewed several studies since 2016 that applied regression methods in radicalization studies using the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START), Profiles of Individual Radicalization in the United States (PIRUS) dataset, that focused on the causal motivations leading to violent attacks by individuals operating under different extremist ideologies. This dataset is considered a comprehensive individual-level dataset that samples 2,226 incidents of individuals from every ideological background ("Islamist, far-right, far-left, single issue") who have radicalized in the U.S., to the point of committing an ideologically motivated activity (violent and non-violent), joining a listed entity, or having association with an extremist organization whose leader has been criminally indicted of an ideologically motivated violent offence (Armstrong et al., 2019).

Hypotheses

The Maasberg et al. (2020) and Whitty (2021) studies offer an anchor point to replicate regression-based research on insider threats. The violent extremist portion of this research is based on a review of past regression studies focused on radicalization that source attribute data from the PIRUS dataset and allows the formation of several hypotheses to test the motivation ("M") component of the theoretical construct.

It is believed that violent extremist insider threats represent a variation of motivational and behavioral attributes when compared to other insider threat studies conducted by Maasberg et al. (2020) and Whitty (2021), and that the specific attribute of grievances against the nation-state, has a greater influence for violent extremist insider threats operating under different ideologies.

Doering et al. (2020) reviewed attack incidents across the extremist ideological spectrum and using multinomial logistic regression found that many individual-level variables did not present significant differences between Islamist, right-wing, and left-wing extremists (Doering et al., 2020). Grace (2018) conducted a study using ordinal logistic regression focused on individuals radicalized to Islamist extremist terrorist ideology and found that generalized group grievance against the U.S. predicted active participation in terrorist attacks in the U.S (Grace, 2018). Based on these

studies, we posit that grievance against the government will be a common prevailing item found among insider threats, irrespective of the specific extremist ideology, and formulate the first hypothesis for testing:

H_1. A violent extremist insider threat is principally motivated by revenge against the nation-state as compared to other insider threats that are motivated by revenge against an employer.

In the context of violent extremist insider threat attacks, revenge may be directed to the insider threat's own organization and other employees working in the organization, or to external targets, that may be the opportunistic targets of violence based on revenge that is motivated by anger with society in general within the nation-state.

This research will also determine if there are other motivational or behavioral characteristics that define a violent extremist insider threat. Maasberg et al. (2020) and Whitty's (2021) research on different insider threats confirmed that other attributes were positively correlated; therefore, there may be other attributes that have a positive correlation with violent extremist insider threats. The magnitude of the effects of these variables, should not be as high as the motivation for revenge against the nation-state, which is the defining variable of this insider threat.

Jasko et al. (2017) used multivariate logistic regression and found that when individuals experience a loss of personal significance, it may result in extremist violence based on a motivation to restore significance. Across the ideological spectrum of extremists, failure at work, rejection in social relationships, and victims of abuse, were positive predictors of violent activity. There was additional evidence that the presence of radicalized individuals within an individual's wider social network increased the likelihood of resorting to violent activity (Jasko et al., 2017). Maasberg et al. (2020) and Whitty's (2021) research on different insider threats also referenced these attributes, and leads us to formulate the following hypotheses:

H_2. If a person experiences a loss of standing at work, then the person will be more likely to participate in violent activity at their place of work.

H_3. If there is a change in familial status, such as a divorce, separation or widower, then this will increase the likelihood of a violent extremist insider threat attack.

H_4. If there is a change in performance at work then this will increase the likelihood of a violent insider threat attack.

Jensen and LaFree (2016) indicate that while qualitative studies over the past decade have focused on radicalization pathways, including psychological processes, small group dynamics, and social movement catalysts, they relied on small case studies. This establishes a weak empirical grounding concerning the characteristics of radicalized individuals who engage in violent activity. Analysis of structured attribute data allows for the generation of causes and effects, and the results of a multivariate logistical regression study of the PIRUS dataset revealed which variables and theoretical perspectives were best at explaining violent behaviors amongst radicalized individuals across the ideological spectrum. Specifically, economic deprivation and low educational attainment are not more common amongst extremists than they were for the general population. Further, drug and alcohol abuse were generally lower, and this finding is consistent across ideologies (Jensen & LaFree, 2016). While substance addiction had a positive correlation to insider threat attacks in the Maasberg et al. (2020) and Whitty (2021) studies, it is posited:

H_5. There is no association between alcohol or drug addiction with violent extremist insider threats.

Varaine (2020) notes that there is mixed evidence concerning the general premise that terrorist activity is motivated by a lack of economic opportunities. Varaine (2020) studied the association of economic deprivation and terrorist activities, and through hierarchical logistic regression analysis, found variation based on ideology, with right-wing extremism more likely during long periods of economic deprivation, left-wing extremism more likely during periods of economic improvement, and Islamist extremist attacks not being affected by collective deprivation (Varaine, 2020). Based on this, it is believed that:

H_6. The violent extremist insider threat is not motivated by a lack of economic opportunities and there is no relationship with income.

Methodology and Results

As this research was focused on studying the underlying violent extremist insider threat motivations and behaviors within the CMO model—similar to the focus of the Maasberg et al. (2020) and Whitty (2021) insider threat studies—the PIRUS radicalization dataset, which is a large-N dataset of categorical and ordinal variables, was used to test the hypotheses statements and empirically measure with the use of logistic regression analysis in StataSE version 16. Five motivational and behavioral attributes (independent variables) of greatest association to participation in violence by extremist insider threats (dependent variable) were assessed, when controlling for employment (a pre-condition for being an insider threat) at the time of an attack (further outlined in Table 1) (University of Maryland, 2018). The descriptive statistics for the attributes used in this study may be found in Table 2.

Limitations

A notable limitation in the PIRUS dataset—unlike the CM-CERT-SEI insider threat dataset—is that there is no specific coding for an insider threat. The sample sourced from the PIRUS dataset will address this by: 1) using the criteria for employment found within the PIRUS attribute of employment status, 2) within this sample, compare violent and non-violent extremist insider threats based on the PIRUS attribute that codes violence at the time of an attack, and, 3) cross-referencing a selection of cases from this violent extremist insider threat sample with publicly available information to confirm its validity as being representative of the sub-population (i.e., insider threat) of interest. Another limitation in the dataset, was the lack of data indicating whether those in the insider threat study had conducted

Table 1. Motivational and Behavioral Attributes of the Violent Extremist Insider Threat (coding and descriptions are from the PIRUS dataset)

	CM-SEI Insider threat dataset with a sample of 74 insider threat cases (Maasberg et al., 2020)	**Interview dataset with a sample of 99 U.K.-based insider threat cases (Whitty, 2021)**	**UM-START PIRUS dataset with a sample of 122 extremist insider threat cases (some attributes required the creation of "dummy" variables)**
Dependent variable	Sabotage (main) Fraud Theft of intellectual property	"Harder times"	**Violent Extremist Insider Threat (*New)**, 0=No, 1=Yes **Criminal Severity**, 3=White-collar crimes/ vandalism is used to approximate fraud and theft behaviors (Note: There were no instances in the dataset of this attribute being coded as a "1-Yes" when the violent attribute was controlled)
Independent variables (Study variables)	**Motive** Revenge (main) Financial gain Personal gain **Behavioral** Addiction Poor performance Supervisor conflict	Family change (divorce)	**Motive** **Angry with U.S. Society**, 0=No, 1=Yes **Adulthood Social Stratum (income)**, 1=Low, receives welfare, lives close to poverty line, 2= Middle, does not receive welfare, has steady professional employment, lives in lower-middle or middle class neighborhood, and 3= High, works a high income, white-collar job, lives in middle or upper class neighborhood **Social Standing**, diminution prior to radicalization?, 0=No, 1=Yes, at different points of the radicalization process **Marital Status**, change at the date of exposure, 0=No, as they were either single or married, 1=Yes, as they were divorced, separated, or widowed **Behavioral** **Alcohol or Drug Abuse**, 0=No, 1=Yes **Change in Performance at Work**, 0=No, 1=Yes *There was no attribute in PIRUS that could approximate supervisor conflict; however, it is assumed that a change in work performance resulted in conflicts with supervisors (Note: this attribute was ultimately dropped from the regression model as there were not enough observations)
Control variables	*To be considered a violent extremist insider threat attack; the subject(s) of an observation must be employed and conduct a violent attack that is informed by an ideological radicalization; however, there is variability in terms of target (internal or external to the workplace) selection. Additional regression models considered the impact of ideological radicalization on attributes' association to insider threat.		**Violent**, participation in ideologically motivated actions, or charged with conspiracy, 0=No, 1=Yes **Employment Status, at the time of exposure**, 0=No, self-employed, unemployed, student, or retiree, 1=Yes, employed **Islamist Radicalization**, 0=No, 1=Yes **Far-Right Radicalization**, 0=No, 1=Yes **Far-Left Radicalization**, 0=No, 1=Yes **Single-Issue Radicalization**, 0=No, 1=Yes

All of the motivational and behavioral attributes listed in the table that are sourced from the PIRUS dataset are anchored against the approximate equivalent attributes from the Maasberg et al. (2020) and Whitty (2021) studies. A smaller N-sample was established based on these selection criteria, and within this sample, insider threat cases were confirmed through cross-referencing of publicly available sources—effectively creating a violent extremist insider threat "N" sample. This sample was examined to determine if there were different strengths of associations between the violent extremist insider threat (dependent variable) with the independent motivational and behavioral variables in the table (122 cases with full attribute data was used in the regression model). The violent extremist insider threat is believed to have more prominent attributes not present in other insider threats researched in the Maasberg et al. (2020) and Whitty (2021) studies that focused on cyber-sabotage, fraud, and IP theft. Revenge motivation (i.e., anger towards the U.S.) is more relevant for the violent extremist insider threat than other motivational and behavioral attributes.

attacks against their own place of employment (causing potential injury to several assets within the insider threat's place of employment including property, information, personnel) vs. other organizations (causing potential reputa-

Table 2. Descriptive Statistics for Main Attributes used in the Study (from the PIRUS dataset)

Attributes	*n*	% of dataset sample
Violent	2226	100
No	935	42
Yes	1291	58
Angry US	1362	61.19
No	416	30.54
Yes	946	69.46
Social Stratum (income) Adulthood	1092	49
Low	273	25
Middle	687	62.91
High	132	12.09
Social Standing (dummy recode)	505	22.6
No	406	80.4
Yes	99	19.6
Marital Status (dummy recode)	1368	61.5
No	1231	89.99
Yes	137	10.01
Alcohol or Drug Abuse	2226	100
No	1976	88.77
Yes	250	11.23
Employment Status (dummy recode)	1070	48
No	508	47.48
Yes	562	52.52
Islamist Radicalization	2226	100
No	1715	77.04
Yes	511	22.96
Far-Right Radicalization	2226	100
No	1249	56.11
Yes	977	43.89
Far-Left Radicalization	2226	100
No	1852	83.20
Yes	374	16.80
Single-Issue Radicalization	2226	100
No	1862	83.65
Yes	364	16.35

Note. N = 2,226

tional damage to insider threat's present place of employment), as all that was indicated was the U.S. city and state (or foreign nation-state) of the extremist activity (University of Maryland, 2018).

Approach

With the use of logistic regression analysis, the extremist insider threat sample was assessed using motivation and behavioral attributes sourced from the PIRUS database that are relevant to insider threats as guided by the Maasberg et al. (2020) and Whitty (2021) studies. While attributes were located for the regression model based on their theoretical relevancy, some were omitted from the study as their inclusion resulted in the loss of a significant number of observations as not every observation contained a full set of attributes. From the original PIRUS dataset of 2,226 observations, selecting motivation and behavioral attributes in this manner to use in the regression model—five in total that are formulated as independent variables—resulted in a comparatively small sample of 232 observations, (122 employed extremist observations and 110 that were not employed). The employment control variable was used to limit the sample to a specific group of interest (i.e., insider threats). The 122 employed extremist observations are the basis for the extremist insider threat sample used in the regression analysis. Further details on this approach may be found in Tables 1 and 2. Another result of this research was the creation of a new attribute within the dataset that

was coded as extremist insider threat. Missing data that were coded in the PIRUS dataset as "-99" were dropped so that these values would not affect subsequent calculations. Non-applicable data that were coded in the PIRUS dataset as "-88" were dropped so that these values would not affect subsequent calculations, after a verification that the data had no theoretical relevancy.

The research used the following base equation for regression modeling:

(Violent Extremist Insider Threat) Attack = B_0 + B_1(Angry with U.S. Society) + B_2(Adulthood Social Stratum) + B_3(Social Standing) + B_4(Marital Status) + B_5(Alcohol or Drug Abuse) + ε_i

As the dataset was qualitative in nature, some of the variables that were used in the estimating equations were recoded into new dichotomous "dummy" attributes to isolate a given attribute's effect on violent extremist insider threat activity. The "logit" command was used in Stata to run the model which had a dichotomous dependent variable, and odds ratios were reported to display marginal effects and express the probabilities of a violent extremist insider threat based on a given attribute. For the dichotomous dependent and independent variables used in the analysis, a "1" value is associated with the attribute being present, and a "0" value is associated with the attribute being not present. As an example, for the study's dependent variable, a violent extremist insider threat, was defined as having "1" values of 1) being violent, and 2) being employed at the time of an attack, within a sample of individuals with extremist ideologies. To verify the validity of the extremist insider threat sample, and that this variable was representative of the population of interest, a selection of the study's 122 sample size of extremist insider threat observations was researched against open sources. It was confirmed that the sample that was used in the regression model (N=122) contained cases such as Nidal Hasan, Alton Nolen, Syed Riswan Farook (all Islamist violent extremist insider threats), Jerad Miller (a far-right violent extremist insider threat associated to Sovereign Citizen), Taylor Michael Wilson (a far-right violent extremist insider threat associated to Identity Evropa), and Richard Preston (a far-right violent extremist insider threat associated to the Ku Klux Klan).

The regression models outlined in Tables 3, 4 and 5 were subjected to robustness and sensitivity diagnostics (results found in Tables A1, A2, and A3 in Appendix), including tests for heteroscedasticity and multicollinearity. A Breusch-Pagan test for heteroskedasticity provided a result of 0.0910, meaning the null hypothesis could be rejected at the 0.10, indicating the presence of mild heteroskedasticity; however, as the dependent variable is binary, and the model is logistic and not linear, this was not an issue in the study. To test for multicollinearity in Stata, the Collinearity Diagnostics package was used to review VIF values. All of the VIFs have values that are under 2 for the base, Islamist, and Far-Right models. It is generally understood that values above 5 indicate that multicollinearity is severe. Based on this, the study is not significantly impacted by multicollinearity occurring in the independent variables.

The robustness tests did not indicate any significant differences in p values for the base model; however, there was some notable variation in p values for statistically significant attributes of adulthood social stratum (i.e., income) when the model was conditioned for Islamist radicalization, and anger with U.S. society when conditioned for Far-Right radicalization. As well, a stepwise reduction procedure was conducted with attributes that were statistically insignificant for the base regression model and found that the main predictor attributes' coefficients were not sensitive to the removal of extraneous attributes (Table 3). Finally, to assess if the logistic regression models fit with the dataset, sensitivity (positive outcomes) and specificity (negative outcomes) were tested, and the base regression model (as well as those conditioned for Islamist and Far-Right radicalization) correctly classified outcomes better than random chance at 79, 90, and 81% respectively, with figures well above 5%, indicating the effectiveness of the model.

Analysis

The results from the regression model provided insights into the relationship between motivational and behavioral attributes and violent extremist insider threat attacks. Specifically, the findings provide support for H_1, which posits that a violent extremist insider threat is principally motivated by revenge against the nation-state as compared to other insider threats. Contrary to H_6, that the violent extremist insider threat is not motivated by lack of economic opportunities, the regression model displayed a statistically significant relationship between lower levels of income and violent extremist insider threats. The analysis did not provide support for H_2, H_3, and H_4, as there were no associations found between loss of standing at work, change in familial status, or decreased performance at work with violent insider threat attacks. Finally, the results supported H_5, and displayed no association between alcohol or drug addiction with violent extremist insider threat activity.

Based on the theoretical model, it would be expected in the regression analysis, that there would be a strong association of true values between violent extremist insider threats and anger with U.S. society. As the regression model employs a dichotomous dependent variable, the analysis sought to examine the probability of a positive outcome in consideration of a set of regressors, while odds ratios are reported as it allows for an interpretation of the relative odds of the occurrence of the outcome of interest, in this case, the probabilities of a violent extremist insider threat based on a given attribute.

In Table 3, there are two statistically significant results related to positive and negative estimated coefficients c). This provides validity to H_1 that violent extremist insider threats' motivation, is informed by anger towards the nation-state as anger with U.S. society increases the risk of violence by 2.7 times. However, contrary to H_6, a lower income increases the risk of violence by 6 times. Unlike the results from the Maasberg et al. (2020) study that examined cyber sabotage, fraud, and IP-theft insider threats, there were statistically insignificant associations between violent extremist insider threats with loss of standing at work, and

Table 3. Extremist Insider Threat Attributes (N =122)

Violent Employed Extremist	Coef.	St. Err.	OR	p-value	[95% Conf	Interval]	Sig
Angry with U.S. Society	1.021782	.4431036	2.77814	0.021	.1533146	1.890249	**
Adulthood Social Stratum (income)	-1.854823	.5621488	.1564807	0.001	-2.956614	-.7530314	***
Social Standing	.985447	.6384776	2.679009	0.123	-.2659461	2.23684	
Marital Status	1.599528	1.116181	4.950697	0.152	-.5881462	3.787203	
Alcohol or Drug Abuse	-.1043307	.6407259	.9009273	0.871	-1.36013	1.151469	
Constant	3.269712	1.17313	26.30375	0.005	.970419	5.569004	***

One-tailed test significance levels = (*p < 0.10), **p < 0.05, ***p < 0.01), LR chi2(5) = 32.63***, Prob > chi2 = 0.0000, Pseudo R2 = 0.2031

Table 4. Violent Islamist Insider Threat

Violent Employed Extremist	Coef.	St. Err.	OR	p-value	[95% Conf	Interval]	Sig
Angry with U.S. Society	3.120792	1.014373	22.66432	0.002	1.132657	5.108927	***
Adulthood Social Stratum (income)	-2.262867	1.22367	.1040518	0.064	-4.661216	.1354831	*
Social Standing	1.320437	1.355391	3.745057	0.330	-1.336081	3.976955	
Marital Status	0	(omitted)	1				
Alcohol or Drug Abuse	-1.00499	1.263152	.3660485	0.426	-3.480721	1.470742	
Constant	3.144371	2.625095	26.30375	0.231	-2.000721	8.289462	

One-tailed test significance levels = (*p < 0.10), **p < 0.05, ***p < 0.01), Number of Observations = 47, LR chi2(4) = 22.19***, Prob > chi2 = 0.0002, Pseudo R2 0.4003

Table 5. Violent Far-Right Insider Threat

Violent Employed Extremist	Coef.	St. Err.	OR	p-value	[95% Conf	Interval]	Sig
Angry with U.S. Society	1.966764		7.147509	0.071	-.1678721	4.1014	*
Adulthood Social Stratum (income)	-2.016545		.1331146	0.106	-4.460328	.4272385	
Social Standing	.8647401		2.374389	0.521	-1.775266	3.504747	
Marital Status	0	(omitted)	1				
Alcohol or Drug Abuse	.4496688		1.567793	0.745	-2.25945	3.158788	
Constant	3.576315		35.7416	0.155	-1.353059	8.505689	

One-tailed test significance levels = (*p < 0.10), **p < 0.05, ***p < 0.01), Number of Observations = 28, LR chi2(4) = 9.11*, Prob > chi2 = 0.0585, Pseudo R2 = 0.2590

alcohol or drug abuse, and when compared to the Whitty (2021) study, a change in familial status was also statistically insignificant.

A further moderation analysis was conducted to test if the strength of association for anger towards U.S. society and income varied depending on ideology. Additional regressions were conducted using this model with different samples using dummy variables conditioned on specific ideological radicalization paths (Islamist, Far-Right, Far-Left, Single-Issue) to determine if there were variation on the effects of a given attribute. Only Islamist and Far-Right radicalization achieved statistically significant result and are further discussed.

What is interesting is that for violent Islamist extremist insider threats, there are significantly stronger estimated coefficients in terms of anger with U.S. society (positive association) and income (negative association) attributes. Being angry against the U.S. increases the risk of insider threat violence by 22 times when Islamist radicalization is involved. Far-right extremist insider threats have similar results, although relatively weaker than Islamist extremists, with anger towards the U.S. still increasing the risk of violence by 7 times.

Limitations, Discussion, Future Avenues for Research and Policy Recommendations

There are additional limitations of this research that should be noted. The PIRUS dataset is not a comprehensive sample of all occurrences of radicalization in the U.S. and may not be a representative sample given its reliance on publicly available information relating to individuals that

have been arrested, charged, and/or indicted with ideological motivated criminal activities, and limited access to historical data sources from the 1940s to the 1980s creating a disproportionate amount of more recent cases in the dataset. Also, there are a significant number of observations that are missing data. This was addressed by PIRUS researchers via the following techniques: simple imputation using fixed values (i.e., cold-deck), sub-group means, regression-based, and expected maximization calculations-based multiple imputation. Finally, researchers who use the dataset are cautioned that studies based on PIRUS are best not utilized to predict radicalization based on indicators as there was no available control group. This is similar in practice to insider threat studies that are based on motivational and behavioral attribute data; rather than "prediction," research studies are meant to identify attributes that appear to be more causally related to specific insider threats through confirmed past occurrences of insider threat attacks.

There are several limitations when using categorical or discrete data as predictor variables. These were considered in the present study when choosing independent variables based on their theoretical relevancy, and testing for multicollinearity, along with restricting the number of overall independent variables (Ranganathan et al., 2017). It should be noted that the outcomes are not evenly split in the samples, with 77 (63%) of the observations being associated to violence in the base regression model, along with 34 (72%), and 19 (68%) of violence observations found in those regression models conditioned for Islamist and Far-Right radicalization. To overcome the limitations in logistic regression, applying qualitative comparative analysis (QCA) will be considered in the future to augment the present research study.

The sample size used in certain models within this study is another limitation. Of the 28 observations used in the Far-Right regression model, 19 far-right insider threats were violent, and nine were not. While this small sample size is problematic and gaining access to real case data is a present limitation in the field of insider threat research as a whole, this study as an exploratory analysis still provides value and insight as the findings provide suggestive relationships that require additional follow-up study. Further, as previously mentioned, the VIF has values that are under 2 for the Far-Right model, indicating that it is not significantly impacted by multicollinearity occurring within the independent variables.

Another significant limitation is whether the attributes associated to the violent extremist insider threat from this research study would hold true if the sample included incidents from other nation-states. As anger towards the U.S. as an attribute in PIRUS was defined as public statements opposing public policies, destroying symbolic U.S. items, or promoting inflammatory U.S. messages (University of Maryland, 2018), would a violent extremist insider threat in Canada for example be characterized by opposition to Canadian government policies and against Canadian society in general, or, in this example could insider threat attacks also be done to demonstrate opposition to another nation-state's policies (such as the U.S.). It would also seem plausible for violent extremist insider threats to not necessarily have a grievance against their own nation-state and to conduct an attack in demonstration of solidarity to a trans-national extremist cause or listed entity (e.g., Islamic State being opposed to Western nation-states in general, Sovereign Citizens/Freeman-on-the-Land displaying similarities across the U.S./Canadian border).

Figure 1. Insider Threat Causal and Conditional Mechanism Model

In conclusion, based on the results of this study, in terms of statistical significance, the violent extremist insider threat does demonstrate unique motivational attributes, specifically, anger with U.S. society and lower levels of income. These attributes are even more relevant when considering Islamist and Far-Right radicalization.

In terms of policy relevance and security risk mitigation, this provides rationale that enhanced monitoring controls to detect potential extremist threats are justified as there are specific attributes, at least in the U.S. context concerning domestic extremists, which could be detected in sentiment exposed in employees' social media (Park et al., 2018), given that the workplace monitoring of Internet usage has been outlined as useful in determining if there is a potential threat to the organization (Rausch, 2021).

A follow-up regression research study could determine if there are additional motivational and behavioral attributes which may be statistically relevant to this insider threat. Also, by combining qualitative QCA methods, analyzing additional incident details from the regression base model sample of 122 insider threats from the PIRUS dataset could confirm the conditional mechanisms related to attacks given the interesting variation in terms of target selection from several of the observations found in the sample. For example, as all violent extremist insider threats in this sample were employed at the time of an attack, why did target selection sometimes occur outside the place of employment? This suggests that there may be additional motivational and behavioral attributes that are specific to each outcome, as well as organizational policy and program insider risk mitigation controls to be considered, as detailed in the following causal and conditional mechanism model (Figure 1).

It is a further goal of the research to apply the methodological approach and insider threat presented in this paper to other datasets in the future, including other countries' datasets capturing real insider threat compromises, to continue to enhance the reliability and validity of the overall study.

Submitted: October 10, 2022 PDT. Accepted: April 28, 2025 PDT. Published: May 12, 2025 PDT.

Table 6. Descriptive Statistics for Main Attributes used in the Main Regression Model Sample

Attributes of employed extremists	*n*	% of regression sample
Violent	122	100
No	45	36.89
Yes	77	63.11
Angry US	122	100
No	42	34.43
Yes	1	65.57
Social Stratum (income) Adulthood	122	100
Low	25	20.49
Middle	86	70.49
High	11	9.02
Social Standing (dummy recode)	122	100
No	96	78.69
Yes	26	21.31
Marital Status (dummy recode)	122	100
No	111	90.98
Yes	11	9.02
Alcohol or Drug Abuse	122	100
No	102	83.61
Yes	20	16.39
Employment Status (dummy recode)	122	100
No	0	0
Yes	122	100
Islamist Radicalization	122	100
No	73	59.84
Yes	49	40.16
Far-Right Radicalization	122	100
No	89	72.95
Yes	33	27.05
Far-Left Radicalization	122	100
No	107	87.70
Yes	15	12.30
Single-Issue Radicalization	122	100
No	97	79.51
Yes	25	20.49

Note. $N = 122$ (employed extremists)

References

Armstrong, G., Derrick, D., Hienz, J., Ligon, G., & Southers, E. (2019). *Characteristics of homegrown violent extremist radicalization*. National Center for Risk and Economic Analysis of Terrorism Events University of Southern California.

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

Bell, A. J. C., Rogers, M. B., & Pearce, J. M. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*, *24*, 166–176. https://doi.org/10.1016/j.ijcip.2018.12.001

Cassidy, T. (2017, December 11). *Technical detection of intended violence: Workplace violence as an insider threat*. Carnegie Mellon Software Engineering Institute. http://insights.sei.cmu.edu/blog/technical-detection-of-intended-violence-workplace-violence-as-an-insider-threat/

Cassidy, T., Gardner, C., Miller, S., & Moore, A. P. (2018). *Analyzing incidents of workplace violence to inform incident planning and mitigation strategies*. Defense Technical Information Center. https://apps.dtic.mil/sti/citations/AD1090846

Centre for the Prevention of Radicalization Leading to Violence. (2016). *Radicalization leading to violence in the workplace*. https://www.wissenschaftsinitiative.at/rad/database/centre-for-prevention/

Cybersecurity, U. S. & Infrastructure Security Agency. (2020). *Insider threat mitigation guide*. United States Department of Homeland Security.

Dearden, L. (2020, March 5). *"Neo-Nazi" metropolitan police officer arrested on suspicion of terror offences*. Independent. http://www.independent.co.uk/news/uk/crime/police-officer-terror-arrest-met-london-right-wing-group-a9379641.html

Doering, S., Sara, D., Garth, C., & Raymond. (2020). Reconceptualizing ideology and extremism: Toward an empirically based typology. *Studies in Conflict and Terrorism*, *13*, 17.

Grace, E. (2018). Lex talionis in the twenty-first century: Revenge ideation and terrorism. *Behavioral Sciences of Terrorism and Political Aggression*, *10*(3), 249–263. https://doi.org/10.1080/19434472.2018.1428660

Ho, S. M., Kaarst-Brown, M., & Benbasat, I. (2018). Trustworthiness attribution: Inquiry into insider threat detection. *Journal of the Association for Information Science and Technology*, *69*(2), 271–280. https://doi.org/10.1002/asi.23938

Jasko, K., LaFree, G., & Kruglanski, A. (2017). Quest for significance and violent extremism: The case of domestic radicalization. *Political Psychology*, *38*(5), 815–831. https://doi.org/10.1111/pops.12376

Jensen, M., & LaFree, G. (2016). *Final report: Empirical assessment of domestic radicalization (EADR)*. National Consortium for the Study of Terrorism and Responses to Terrorism. https://www.start.umd.edu/publication/empirical-assessment-domestic-radicalization-eadr

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A. M. (2018). *Insider threat detection study*. North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/library/publications/insider-threat-detection-study/

Lowenthal, M. M. (2002). *Intelligence: From secrets to policy*. Congressional Quarterly Press.

Maasberg, M., & Beebe, N. L. (2014). The enemy within the insider: Detecting the insider threat through addiction theory. *Journal of Information Privacy and Security*, *10*(2), 59–70. https://doi.org/10.1080/15536548.2014.924807

Maasberg, M., Zhang, X., Ko, M., Miller, S. R., & Beebe, L. N. (2020). An analysis of motive and observable behavioral indicators associated with insider cyber-sabotage and other attacks. *IEEE Engineering Management Review*, *48*(2), 151–165. https://doi.org/10.1109/EMR.2020.2989108

Mekonnen, S., Padayachee, K., & Meshesha, M. (2015). A privacy preserving context-aware insider threat prediction and prevention model predicated on the components of the fraud diamond. *Annual Global Online Conference on Information and Computer Technology, IEEE*, 60–65. https://doi.org/10.1109/GOCICT.2015.20

Mills, J. U., Dever, J. R., & Stuban, S. M. F. (2018). Using regression to predict potential insider threats. *Defense Acquisition Research Journal*, *25*(2), 122–157. https://doi.org/10.22594/dau.16-771.25.02

National Institute of Justice. (2015). *Radicalization and violent extremism - Lessons learned from Canada, the U.K., and the U.S.* United States Department of Justice. https://www.ojp.gov/ncjrs/virtual-library/abstracts/radicalization-and-violent-extremism-lessons-learned-canada-uk-and

Ornatowski, C. M., & Pottathil, A. (2012). Digital communications surveillance: A challenge for rhetoric studies. *African Yearbook of Rhetoric*, *3*(1), 17.

Park, W., You, Y., & Lee, K. (2018). Detecting potential insider threat: Analyzing insiders' sentiment exposed in social media. *Security and Communication Networks*, 1–8. https://doi.org/10.1155/2018/7243296

Pugliese, D. (2020, October). *Canadian Forces push-back against Proud Boys and far right needs action, not tweets, critics say*. Ottawa Citizen. https://ottawacitizen.com/news/national/defence-watch/canadian-forces-pushback-against-proud-boys-and-far-right-needs-action-not-tweets-critics-say

Ranganathan, P., Pramesh, C. S., & Aggarwal, R. (2017). Common pitfalls in statistical analysis: Logistic regression. *Perspectives in Clinical Research*, *8*(3), 148–151. https://doi.org/10.4103/picr.PICR_87_17

Rausch, S. L. (2021, April 7). Preparing for extremism in the workplace. *Security Magazine*. https://www.securitymagazine.com/articles/94973-preparing-for-extremism-in-the-workplace

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counterintelligence*, *26*(3), 453–481. https://doi.org/10.1080/08850607.2013.780552

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organizations. *Journal of Information Security and Applications*, *40*, 247–257. https://doi.org/10.1016/j.jisa.2017.11.001

Sahinkaya, E. (2020, August 1). *Germany dissolves elite army unit over far-right activity*. VOA News. https://www.voanews.com/extremism-watch/germany-dissolves-elite-army-unit-over-far-right-activity

Schoenherr, J. R., & Thomson, R. (2020). Insider threat detection: A solution in search of a problem. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–7. https://doi.org/10.1109/CyberSecurity49315.2020.9138862

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security*, *21*(6), 526–531. https://doi.org/10.1016/S0167-4048(02)01009-X

Shulsky, A. N. (1991). *Silent warfare: Understanding the world of intelligence*. Brassey's Book Company.

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

University of Maryland. (2018). *Profiles of individual radicalization in the United States (PIRUS) codebook*. National Consortium for the Study of Terrorism and Responses to Terrorism. https://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus

Van Evera, S. (1997). *Guide to methods for students of political science*. Cornell University Press.

Van Os, E., Gips, M., Stewart, S., & LeTellier, V. (2021). *Political extremism and insider threat early warning*. ASIS Global Security Exchange. https://www.gsx.org/gsx-blog/political-extremism-and-insider-threat-early-warning/

Varaine, S. (2020). Revisiting the economics and terrorism nexus: Collective deprivation, ideology and domestic radicalization in the US (1948–2016). *Journal of Quantitative Criminology*, *36*(3), 667–699. https://doi.org/10.1007/s10940-019-09422-z

Wang, J., Gupta, M., & Rao, H. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91–112. https://doi.org/10.25300/MISQ/2015/39.1.05

Whitty, M. T. (2021). Developing a conceptual model for insider threat. *Journal of Management and Organization*, *27*(5), 911–929. https://doi.org/10.1017/jmo.2018.57

Appendix

Regression Models' Diagnostics (robustness)

Table A1. Extremist Insider Threat

Violent Employed Extremist	Coef.	OR	p-value	p-value(robust std. err.)
Angry with U.S. Society	1.021782	2.77814	0.021	0.019
Adulthood Social Stratum (income)	-1.854823	.1564807	0.001	0.001
Social Standing	.985447	2.679009	0.123	0.115
Marital Status	1.599528	4.950697	0.152	0.180
Alcohol or Drug Abuse	-.1043307	.9009273	0.871	0.868
Constant	3.269712	26.30375	0.005	0.004

One-tailed test significance levels = (*p < 0.10), **p < 0.05, ***p < 0.01), Number of Observations = 122, LR chi2(5) = 32.63***, Prob > chi2 = 0.0000, Pseudo R2 = 0.2031

Table A2. Islamist Insider Threat

Violent Employed Extremist	Coef.	OR	p-value	p-value (robust std. err.)
Angry with U.S. Society	3.120792	22.66432	0.002	0.003
Adulthood Social Stratum (income)	-2.262867	.1040518	0.064	0.028
Social Standing	1.320437	3.745057	0.330	0.193
Marital Status	0	1		
Alcohol or Drug Abuse	-1.00499	.3660485	0.426	0.379
Constant	3.144371	26.30375	0.231	0.175

One-tailed test significance levels = (*p < 0.10), **p < 0.05, ***p < 0.01), Number of Observations = 47, LR chi2(4) = 22.19***, Prob > chi2 = 0.0002, Pseudo R2 0.4003

Table A3. Right-Wing Insider Threat

Violent Employed Extremist	Coef.	OR	p-value	p-value(robust std. err.)
Angry with U.S. Society	1.966764	7.147509	0.071	0.050
Adulthood Social Stratum (income)	-2.016545	.1331146	0.106	0.157
Social Standing	.8647401	2.374389	0.521	0.497
Marital Status	0	1		
Alcohol or Drug Abuse	.4496688	1.567793	0.745	0.717
Constant	3.576315	35.7416	0.155	0.250

One-tailed test significance levels = (*p < 0.10), **p < 0.05, ***p < 0.01), Number of Observations = 28, LR chi2(4) = 9.11*, Prob > chi2 = 0.0585, Pseudo R2 = 0.2590