This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0836

Analyzing Incidents of Workplace Violence to Inform Incident Planning and Mitigation Strategies

Tracy Cassidy
CERT National Insider Threat Center
Carnegie Mellon University
Software Engineering Institute
Pittsburgh, Pennsylvania
tmcassidy@cert.org

Carrie Gardner
CERT National Insider Threat Center
Carnegie Mellon University
Software Engineering Institute
Pittsburgh, Pennsylvania
cgardner@cert.org

Sarah Miller
CERT National Insider Threat Center
Carnegie Mellon University
Software Engineering Institute
Pittsburgh, Pennsylvania
semiller@cert.org

Andrew P. Moore
CERT National Insider Threat Center
Carnegie Mellon University
Software Engineering Institute
Pittsburgh, Pennsylvania
apm@cert.org

***Abstract*—The National Insider Threat Center (NITC), part of the Software Engineering Institute's CERT Division, has expanded the scope of insider threats to encompass workplace violence (WPV) risk including harm to self and/or others. With this change, we sought to establish a robust data collection and analysis process, like the one we developed for traditional insider threats, to facilitate empirical research in this domain and help produce reliable, high-fidelity findings and artifacts. This work presents our initial analysis and insight. We describe the data collection and analysis process and notate our preliminary artifacts such as a WPV incident chronology, we document initial steps for monitoring and measuring WPV indicators, and we discuss the related privacy, ethical, and legal considerations. We intend this work to catalyze the empirical investigation into the socio-technical problem of mitigating WPV risk. We find that this problem requires operational controls and buy-in from the human resources, personnel security, and legal units as well as from the information technology department and the insider threat program.**

Keywords*—*workplace violence, suicide, insider threat, risk management, targeted violence

I. Introduction

The National Insider Threat Center (NITC), part of the Software Engineering Institute's CERT Division, has been researching and providing best practices for the prevention, detection, and mitigation of insider threat for over 17 years. Until recently, this work has focused on national security espionage, cyber sabotage, fraud, and theft of intellectual property. As the scope of insider threat has expanded, so too has our work. Our definition of insider threat [1] has recently expanded to align itself with the shifting government and industry definitions and includes harm to others and/or oneself within the organizational setting. As discussed below, protection of the workforce, a critical asset to the organization, is essential and often mandated.

Several mandates, including the Executive Order (E.O.) 15387 and Department of Defense (DoD) Workplace Violence Prevention and Response Policy Instruction 1438.06, require that all U.S government and military entities and their contractors that employ persons who hold national security clearances maintain an insider threat program to protect against insider threats to critical assets. These critical assets may include facilities, mission, national security secrets and employees. The E.O. also established the National Insider Threat Task Force (NITTF), whose mission is to "deter, detect, and mitigate actions by employees who may represent a threat to national security by developing a national insider threat program with supporting policy, standards, guidance, and training" (The National Counterintelligence and Security Center). As part of that mission, NITTF identifies intervention in potential suicide and workplace violence incidents, as described below:

> *It is critically important to recognize that an individual may have no malicious intent, but is in need of help. We have invested a tremendous amount in our national security workforce and it is in everyone's interest to help someone who may feel he or she has no other option than to commit an egregious act – such as espionage, unauthorized disclosure, suicide, workplace violence, or sabotage. Intervention prior to the act can save an employee's career, save lives, and protect national security information (NITTF Fact Sheet)* [2].

Workplace violence can have serious detrimental consequences to critical infrastructure or any critical operational environment. For the purposes of this work we use OSHA's definition of work place violence, "any physical assault, threatening behavior, or verbal abuse occurring in the work setting" [3]. These instances of WPV incidents include: shootings, stabbings, suicides, threats, and harassment. It is important to note that it is often difficult to ascertain if someone is a threat to themselves, others, or a combination, as is frequently seen in murder-suicide incidents [4].

Despite the interest in preventing workplace violence in both the private and public sectors, there is a lack of technical controls and capabilities designed to prevent, detect, and mitigate workplace violence risk. Traditionally, technical insider threats such as IT sabotage, theft of intellectual property (IP), unauthorized disclosure, fraud, and espionage are monitored using User Activity Monitoring (UAM) and User-Entity Behavioral Analytics (UEBA/UBA) solutions. However, despite the volume of data these tools collect, most insider threat monitoring solution stacks are still in their infancy in terms of utilizing behavioral or non-traditional technical data sources such as human resource records. This behavioral data is valuable for technical insider threats and *essential* for workplace violence threats, where the only manifestations of predicate indicators may be behavioral [5]. It is pivotal for the research community to investigate the threats of intended physical harm by employees and report on findings related to actionable controls to facilitate incident planning and mitigation strategies. Our goal is to address this issue by incorporating, aggregating, and codifying known precursors of workplace violence.

We began the project by identifying and evaluating literature spanning threat assessment, psychology, clinical assessments tools, military standards and reporting, and epidemiology. We identified specific indicators within the research related to harm to others (potential homicidality) and harm to self (self-injurious behaviors or suicide). We further identified indicators that were associated with both homicidality and suicidality. Once we identified primary indicators, they we structured them into a factor tree [6]. This factor tree in turn informed both a high-level, hierarchical representation of these indicators, called the Pathway to Harm, and the development of threat scenarios. After indicators were integrated into the pathway, we identified discrete manifestations of each indicator and paired them with both associated data sources and implementation guidance. We also identified which indicators may pose challenges in implementation due to regulatory and privacy concerns.

We begin by discussing the relevant literature on suicidality and homicidality, referencing specific assessment tools and studies that informed our development of indicators and models. Next, in developing the factor tree, we complement this research with incident analysis of 26 cases of workplace violence. Using both the established literature and case analysis, we developed the Pathway to Harm model (see Figure 1), a hierarchical depiction of indicators associated with homicidality and/or suicidality. In generating threat scenarios, we discuss a proposed typology for conceptualizing a subset of threats on the spectrum of homicidality to suicidality.

We then describe technical and socio-technical considerations for indicator development and implementation. We examine the limitations of this work given our focus on simulated data. We lastly propose future work that includes testing of indicators and insider threat tools in a virtual network-based simulation environment housed in the CERT NITC.

II. Related Research

The review of the literature spanning a multi-disciplinary field gave us a fuller understanding of what the indicators of suicidal ideation and intent are as well as indicators of targeted or intended violence. Indicators included both the Columbia-Suicide Severity Risk Scale (C-SSRS) [7] for suicidality, the Macarthur Violence Risk Assessment Study [8], and the Workplace and Violence Risk Assessment (WAVR-21) [9]for workplace violence as well as many other works referenced in the Department of Defense Suicide Event Report (DoDSER) [10] and Army STARRS work on behavioral based predictors of workplace violence [10].

The difference between clinical and technical tools, when attempting to detect if an individual is at risk, is that the latter requires the monitoring of technical or cyber systems to gather information, rather than an in-person assessment where one would gather information directly from the individual and require consultation with a mental health professional. Insider threat programs should consult their legal, civil rights, and behavioral health teams when determining monitoring and follow-up protocols.

There has been a great deal of research on textual analysis of social media posts [11] [12] [13]. Linguistic analysis is a powerful tool that can augment the capability of insider threat detection tools and will be discussed further in the Future Research section of this paper. However, due to the breadth of this research, we decided to focus strictly on behavioral indicators.

III. Incident Analysis [12]

A. Data Collection

We reviewed 26 coworker-on-coworker workplace violence incidents that took place between 1986 and June 2017. The incidents selected were chosen based on the overall impact of the incident (in terms of victim count) and availability of information on the subject. In every incident, the perpetrator was a current or former employee targeting an employing

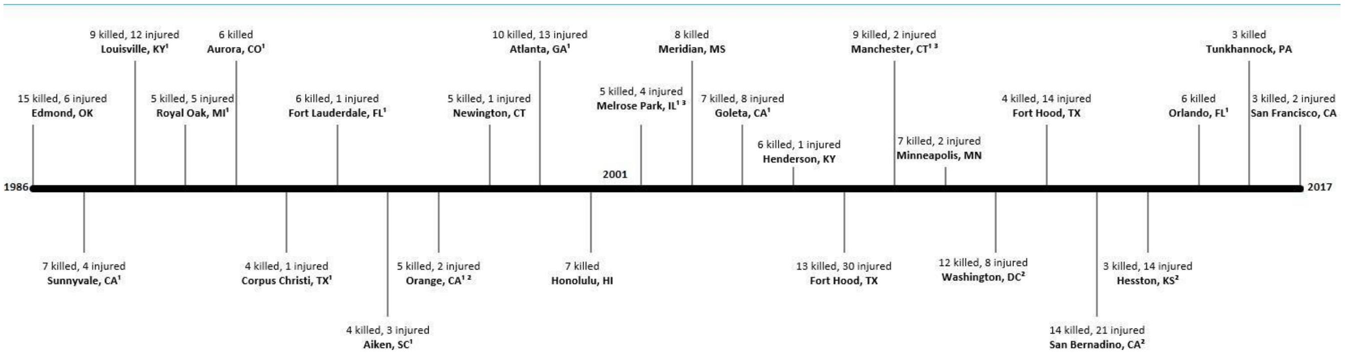
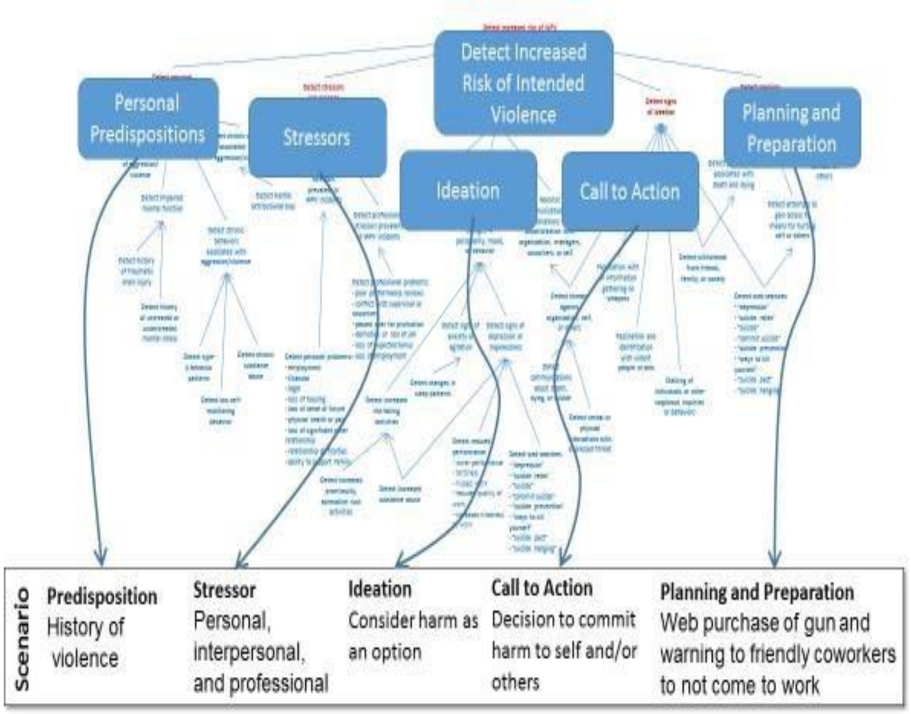


Figure 1: Workplace Violence Timeline

Identify applicable funding agency here. If none, delete this textbox.


Detect Increased Risk of Intended Violence
Personal Predispositions
Stressors
Ideation
Call to Action
Planning and Preparation
Scenario
Predisposition
History of violence
Stressor
Personal, interpersonal, and professional
Ideation
Consider harm as an option
Call to Action
Decision to commit harm to self and/or others
Planning and Preparation
Web purchase of gun and warning to friendly coworkers to not come to work

incidents together on a timeline. In the incidents on the top of the timeline, the insider-perpetrator committed suicide. These incidents include the perpetrator in the fatality total.[2]

Nearly two-thirds (65.4%) of perpetrators identified committed suicide after killing coworkers. Four additional perpetrators (15.4%) were killed in confrontations with police during the incident, which may or may not have been the result of attempts to commit "suicide by cop." Half (50.0%) of all of the perpetrators were former employees at the time of the incident.[3]

We chose not to study or quantify specific workplace suicide-only incidents. Considering that not all workplace suicides are reported in the public media, we were concerned that any incidents that were reported would not be representative or have sufficient information. [4] Instead, we focused on indicators identified in the relevant literature and the frequency of suicide within the sample of workplace homicide incidents.

B. Factor Tree

In the analysis of our collected cases, we identified many contributing factors that were relevant to different case types. In our attempt to construct models of various aspects and causal components of workplace violence and suicidality, we organized the contributing factors into a *factor tree* to present the relationships and categorize dependent factor types [6]

This factor tree, presented in **Error! Reference source not found.**, shows how in analyzing the contributing major and minor factors and the dependencies between the variables, we identified five major categories of contributing factors: Personal Predispositions, Stressors, Ideation, Call to Action, and Planning and Preparation. We will describe these in detail in the Chronology section.

C.Chronology

In evaluating the factor tree, we observed the temporal pattern of the major categories. Upon evaluating the factor tree, we found the identified classes align with the related literature in the Pathway to Violence [14] and Critical Pathway [15] [16]work. Those models capture the temporal observations and factors that contribute to an individual escalating towards harm or violence. The chronology serves as a temporal taxonomy.

In the same vein, we took the factor tree categories and chronologically arranged them to formulate the Chronology of Harm presented in **Error! Reference source not found.**.

The Factor Tree represent potential risk indicators of WPV and are not meant to be visible in this diagram.

D. Pathway to Harm

The Pathway to Harm was developed utilizing the Critical Pathway to Insider Risk [15] [16], which was developed at the

[1] The San Bernardino, CA incident is the only one in which the primary perpetrator, a current employee, had an accomplice.

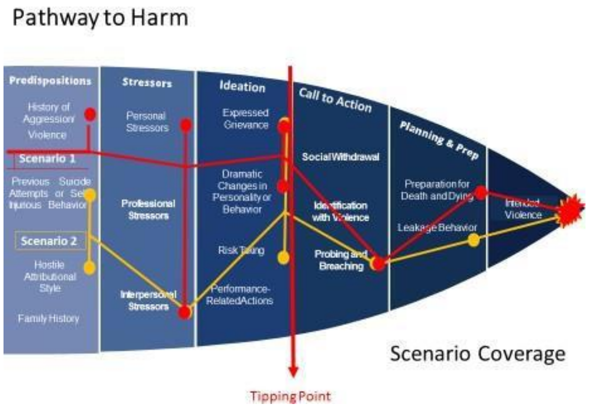
[2] For the Atlanta, GA and Goleta, CA incidents, the number of victims does not include additional fatalities unrelated to the workplace. In both of these incidents, the perpetrator killed individual(s) prior to committing work-related homicides.

[3] In the Henderson, KY incident, the perpetrator returned to attack their coworkers immediately after being removed from the premises. It was unclear whether or not the perpetrator had actually been terminated. Similarly, in the Minneapolis, MN incident, the perpetrator was aware that they would be told that they were going to lose their job. For that reason, the perpetrator brought a firearm to enact revenge against their supervisor and other coworkers.

[4] Suicides tended to be reported in conjunction with coworker-on-coworker violence.

CERT NITC in collaboration with Dr. Eric Shaw. The Critical Pathway was not developed to specifically address issues of workplace violence or suicidality, so we combined that pathway with a well-known pathway for the progression of violence called the Pathway to Violence [14]. To further build our Pathway to Harm, we also utilized Meloy et. al's [17] warning behaviors for potential workplace violence. Finally, we overlaid indicators of self-harm that were not cross-over indicators with indicators of violence. In compilation, these indicators provided the ability to group high-level indicators to develop the Pathway to Harm. The Pathway to Harm is not all inclusive; however, it provides an ability to observe the potential progression of imminence in an insider's actions.

Figure 3: Pathway to Harm with Scenario Mapping



The Pathway to Harm is broken into six categories that range in imminence from left to right. As with other pathways, there can be escalation and de-escalation, and progression does not predict an intended act of violence. Personal predispositions, or things that might predispose someone to suicidal and/or homicidal ideations, are compounded by stressors such as divorce, death of a loved one, issues in the workplace, and conflicts with friends, family, or coworkers. As someone progresses down the pathway, they may have ideations, or thoughts that begin to formulate, that they may be able to utilize harm to self and/or others to mitigate their feelings of unease. This is referred to the "Could Do" stage of the pathway. The tipping point to potential action occurs in what we refer to as the "Call to Action" or "Would Do" stage, where one decides that action to mitigate their situation is necessary. During the "call to action" phase, more significant changes in behavior and thoughts may occur and may be detectable on some level by coworkers. The final stage prior to the act of intended harm is a preparatory stage, during which one may prepare for death by selling belongs, saying goodbye to loved ones, and writing wills or manifestos. Leakage behavior, one of Meloy et. al's [17] warning behaviors, occurs when someone communicates to a third party their intent to harm a target. This communication is not always forthright; however, it often occurs via technological means, which enables it to be detected via insider threat detection tools. Finally, if one moves to the final phase of the pathway, imminent harm is to be expected and may take the form of harm to others and/or oneself.

Figure 3 presents two distinct scenarios of a workplace violence event. Scenario 1 (red line) begins with an individual with a history of aggression or violence (e.g., domestic violence arrest). The subject is then exposed to personal stress (e.g., bankruptcy) and begins to express characteristics of ideation, such as dramatic changes in personality or behavior and expressed grievances. Internal stress and issues begin to manifest outwardly in the ideation phase, revealing observable markers that are more identifiable. If the ideation advances, the subject typically moves through a "Call to Action" phase where they decide to carry out harmful behavior. This is the tipping point were intervention can take place before the individual further escalates and begins planning the activity. The subject in Scenario 1 conducts probing and breaching activities, such as testing rules to see what the subject can get away with doing. The Scenario 1 subject then prepares for death as part of the plan before committing the actual act of violence.

Scenario 2 (orange line) presents a different hypothetical, where the subject with a history of previous self-harm and a hostile attributional style is exposed to interpersonal stress, which cascades into several manifestations of ideation, proceeds to probing and breaching activity, and concludes with prior leakage behavior (i.e., incidental disclosure of intended harm) before the final violent act.

These two example narratives of workplace violence unfold across a chronology of indicators, illustrating that there are known preceding observables that can be identified as precursors of violent behavior. These observables present opportunities for risk prevention safeguards to impede the escalation and prevent the negative outcomes from occurring.

IV. Practical Findings

For our findings, we wanted to operationalize our analysis into actionable techniques that can be used to create deterrents to prevent workplace violence activity or detection controls to identify early warning indications. This process draws upon existing work in the insider threat domain of developing indicators, planning a monitoring and measurement process, and implementing controls to prevent, detect, and respond to the malicious activity. There are many data sources for the monitoring of employee behavior, performance, and risk in the workplace. The Chronology of Harm led to the development of *indicators*, which include methods for monitoring and measurement. Indicators are *observable events that are associated with a potential increased risk.* Indicators are measurable, actionable, and *imperfect*, particularly when assessing risk employees pose to themselves or others, due to the social and kinetic nature of these phenomena. Not all indicators are useful or reliable, and a process should be in place to evaluate the performance of indicators related to measurement objectives.

In this section, we will present a subset of the indicators that we identified in our analysis, discuss considerations for incorporating such indicators into a monitoring program, and detail how implementation could be operationalized.

We aim for this discussion to facilitate appropriate and valuable monitoring approaches to aid prevention and detection of employee workplace violence and self-injurious behaviors. (We will briefly discuss the limitations of these approaches in *Don't Forget Counsel Considerations*). Implementation of these approaches should be made at the discretion of the organization and based on current workforce needs.

A. *Indicators*

Indicators facilitate monitoring or assessing features that may amplify the threat of harmful activity. Indicators are made *measurable* by monitoring various *manifestations*—predicate observable expressions of an activity associated with a risk event (e.g., domestic violence arrest record or frequently visiting a darknet market website on a company workstation). Manifestations can describe the different representations of an indicator, which can be visible through different media such as technical-only data sources (web proxy logs), behavioral- only data sources (background checks), or technical- behavioral data sources such as electronic communications data (e.g., email records).

Measuring indicators facilitates the collection of evidence, which, when analyzed in accordance with other information, can produce *actionable* intelligence on the strength of a particular risk metric.

1) *Development*

We organized our indicator development through a factor tree model to describe indicative markers, using a chronological perspective as an incident would unfold. The categories of indicators include Predispositions, Stressors, Ideation, Call to Action, Planning & Preparation, and Intended Violence. For every indicator in each category, we elaborated potential manifestations, data sources that can be used for monitoring and measurement, and implementation details to describe a general specification of how to configure generic tools to collect the data. Due to the sensitivity of this topic, we will only disclose a brief example from our findings.

a) Example Potential Risk Indicators

Table 1 shows the potential risk indicators of workplace violence we have identified.

Table 1: Potential Risk Indicators

Indicator	**Observables**	**Data Source**
History of Violence	Battery/assault arrest records	Criminal Records Check
Legal Problems	Bankruptcy, serious indebtedness	Background Check
Loss of Significant Other	Change in status/name	HR Records
Conflicts with Supervisor or Co-workers	HR complaints	HR Records
Potential/Actual Loss of Employment	Demotion, temporary suspension, poor performance review	HR Records
Increased Alcohol Usage	Coming to work drunk or severely hung over	HR Records
Concerning Web Searches	Attempted visits to restricted sites, visits to darknet sites	Web Proxy Logs

This table is only a sample of the indicators identified in this extensive research.

2) *Justification*

Indicators have great impact on high-fidelity risk assessment and employee privacy, so they should be developed and supported by empirical evidence that describes *why* a specific feature is associated as precursors to a risk scenario. This justification should present supporting evidence connecting the indicators, and their manifestations, to identified attributes of the risk model in question—workplace violence in this application. This is particularly true of indicators that relate to potential mental health concerns, which are bound by the Health Insurance Portability and Accountability Act (HIPAA). Documenting this connection both helps to prevent "bad science" related to spurious relationships or heuristic biases and helps to protect organizations worried about infringing on employee privacy.

B. *Monitor & Measure*

To monitor and measure indicator strength, we identify the associated data sources that can be used to see the indicator observables. We also identify an appropriate analytical technique that can process the data to generate high-fidelity alerts. We can describe this process of monitoring and measuring indicator strength as a quadruple statement:

<indicator><observable><data source><analytical technique>

We began this mapping process in Table 1, documenting the indicator, observables, and associated data sources. These relationships are typically one-to-many between indicators and between associated implementation techniques to monitoring and measurement.

C. *Controls*

Controls are the preventive, detective, and mitigation safeguards that decrease risk. For workplace violence risk, these controls span technical, behavioral, and administrative data sources and functions. After identifying indicators and associated monitoring and measurement techniques, controls can be implemented. In the following section we briefly present examples of technical, physical, and administrative controls relative to prevention, detection, and mitigation functions.

Table 2: Workplace Violence Controls

	Technical	**Physical**	**Administrative**

Prevention	Indicator Monitoring Process to Identify Precursors, Sentiment/ Emotion Text Analytic Process, Access Control	Metal detectors, turnstiles, CCV cameras	Employee Conduct Policy, Acceptable Use Policies, EAP Programs, Training and Awareness Programs, Positive Incentives Programs
Detection	Indicator Monitoring to Identify Precursors at the "Tipping Point", Access Control	Alarm systems	Anonymous Reporting
Mitigation	Access Control	Safe rooms, bullet-resistant glass	Crisis Counseling, Coordination with Law Enforcement

a) Prevention is the preferred means of dealing with incidents of employee intended harm. Organizational preventative actions may include implementing positive incentives *[18]* within the organization and providing Employee Assistance Programs (EAP) for further employee support.

b) Detection of these types of threats can occur in several different ways and when taken in combination pose the strongest defense. Detection may come from anonymous reporting, human resources, and technical means.

c) Mitigation occurs when the organization has processes in place that facilitate intervention. Behavioral threats may require organizations to include behavioral specialists in their mitigation teams and require close coordination with local law enforcement.

D. Don't Forget Counsel Considerations

In 1998, the Supreme Court ruled in *Faragher v. City of Boca Raton* and *Burlington Industries v. Ellerth* that employers are liable for the discriminatory actions taken by their employees. Both cases cited Title VII of the Civil Rights Act of 1964, which states that employers cannot discriminate against any individual based on race, color, religion, sex, or national origin. The most important component of these decisions is that employers are still liable for supervisor misconduct even if they did not or could not know about the misconduct. The term for this responsibility is *vicarious liability*. Employers are more likely to be held liable when supervisors or managers (i.e., those employees that can cause employee actions against another employee) are perpetrating the harassment. Though these cases specifically involved workplace sexual harassment, the issue of vicarious liability could similarly apply to incidents that escalate to other forms of violence. What remains unclear is an employer's responsibility to employees whom they have reason to believe are suicidal.

No one indicator is definitive evidence of a threat or a particular kind of threat. Some of the personal predispositions (i.e., criminal history) and stressors associated with harm to self or targeted violence may also be associated with technical insider threat. Likewise, indicators for harm to self and others are in many cases shared [4] . Organizations should consider their own risk appetite or tolerance for both technical insider threat and workplace violence, which require documented policies and procedures for escalating from analysis to intervention. In **Error! Reference source not found.** we illustrate the risk environment any organization faces and several use cases for consideration.

Warning behaviors and indicators of violent offenses could appear hours, days, months, or even years in advance. Indicators may exist or appear across data sources, technical tools, and observations by co-workers or supervisors. Organizations should be aware of external stressors that may impact employees. It is essential to note that the existence of personal predispositions, stressors, and even ideations is not necessarily a reason to deem someone inappropriate for an employment position. If ideation is known, it is suggested that further evaluation takes place with appropriate staff.

V. FUTURE WORK

Future plans for this work include coding and expanding the incident corpus of WPV cases, simulating WPV and scenarios in a testbed to evaluate the performance of tools for monitoring and measuring WPV indicators, and developing more efficacious safeguards to prevent, detect, and mitigate WPV risk.

ACKNOWLEDGMENT

It would not have been possible to address the scope of this work without the insights, expertise, and prior work of many others. We thank Sheila Rosenthal from Software Engineering Institute (SEI) Research Services for her contributions to our research process. We thank the SEI Technical Communications team member, Paul Ruggiero, for his expertise and assistance in editing this abstract. We would like to thank Matthew Collins for his contributions to the project's evolution. We would like to thank Dan Costa, the CERT Division's National Insider Threat Center's Technical Solutions Team Lead, for his ongoing feedback and guidance on this work. The team would also like to thank Dr. John Rozel, MD, MSL, for his review of the early indicators.

This material is based upon work funded and supported by the

Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.
Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.
DM18-0836

VI. References

[1] D. Costa, "CERT Definition of 'Insider Threat' - Updated," 7 March 2017. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html.

[2] National Counterintelligence and Security Center, "National Insider Threat Task Force Mission Fact Sheet," [Online]. Available: https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf. [Accessed 1 May 2018].

[3] Occupational Safety and Health Administration, "Workplace Violence," [Online]. Available: https://www.osha.gov/SLTC/workplaceviolence/recognition.html. [Accessed 1 May 2018].

[4] M. Liem, "Homicide Followed by Suicide: A Review," *Aggression and Violent Behavior,* pp. 153-161, 2010.

[5] P. Davis, W. Perry, R. Brown, D. Yeung, P. Roshan and P. Voorhies, "Using Behavioral Indicators to Help Detect Potential Violent Acts: A Review of the Science Base," RAND Corporation, Santa Monica, 2013.

[6] P. K. Davis, "Primer for Building Factor Trees to Represent Social-Science Knowledge," in *Proceedings of the 2011 Winter Simulation Conference*, 2011.

[7] K. Posner, D. Brent, C. Lucas, M. Gould, B. Stanley, G. Brown, P. Fisher, J. Zelazny, A. Burke, M. Oquendo and J. Mann, New York: Columbia University Medical Center, 2008.

[8] J. Monahan, "Macarthur Violence Risk Assessment Study," in *Encyclopeida of Psychology and Law*, Thousand Oaks, SAGE Publications, Inc., 2008, pp. 468-470.

[9] J. R. Meloy, S. G. White and S. Hart, "Workplace Assessment of Targeted Violence Risk: The Development and Reliability of the WAVR-21," *Journal of Forensic Sciences,* vol. 58, no. 5, pp. 1353-1358, September 2013.

[10] L. Pruitt, D. Smolenski, N. Bush, N. Skopp, T. Hoyt and B. & Grady, "DoDSER Department of Defense Suicide Event Report Calendar Year 2015 Annual Report," National Center for Telehealth & Technology, 2016.

[11] B. W. S. B. P. C. A. P. C. a. C. H. O'Dea, "Detecting Suicidality on Twitter," *Internet Inventions,* pp. 183-188, 2015.

[12] S. P. R. V. S. P. M. C. M. M. B. S. D. V. J. a. S. T. Saleem, " Automatic Detection of Psychological Distress Indicators and Severity Assessment from Online Forum Posts," in *Proceedings for COLING 2012*, Mumbia, 2012.

[13] H. Sueki, "The Association of Suicide-Related Twitter Use with Suicidal Behaviour: A Cross Section of Young Internet Users in Japan," *Journal of Affective Disorders,* pp. 155-163, 2015.

[14] T. Calhoun and S. Weston., Contemporary Threat Management, San Diego Specialized Training Services, 2003.

[15] S. E., A. Cummings, M. Hanley, A. Moore, D. Spooner, J. Tupino and R. Trzeciak, "Insider Threat Conceptual Framework: Groupings and Definitions," restricted use, 2010.

[16] E. &. S. L. Shaw, "Application of the Critical-Path Method to Evaluate Insider Risks," pp. 41-48, June 2015.

[17] J. H. J. G. M. &. J. D. Meloy, "The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology," *Behavioral Sciences and the Law,* 2011.

[18] A. S. J. M. E. M. J. R. D. P. S. C. J. C. M. C. T. V. N. B. P. B. D. P. A. Moore, "The role of Positive Incentives for Reducing Insider Threat," Carnegie Mellon University Software Engineering Institute, Pittsburgh, 2016.

[19] The National Counterintelligence and Security Center, "National Insider Threat Task Force Mission Fact Sheet," [Online]. Available: https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf.

[20] U.S. Bureau of Labor Statistics, "Current Population Survey, Census of Fatal Occupational Injuries," Washington, D.C., 2016.

[21] R. Harris, "Suicide in the workplace," U.S. Bureau of Labor Statistics, 2016.

[22] J. A. Wortman and O. G. Schechter, "Suicide and Violent Cognitions, Emotions, and Behaviors in U.S. Military Personnel," Defense Personnel and Security Research Center, Seaside, 2016.

[23] R. J. Hormant and D. B. Kennedy, "Suicide by police: A proposed typology of law enforcement officer-assisted suicide," *Policing: An International Journal of Police Strategies & Management,* vol. 23, no. 3, pp. 339-355, 2000.

[24] S. S. O'Connor, D. A. Jobes, M. Yeargin, M. E. FitzGerald, V. M. Rodriguez, A. K. Conrad and T. W. Lineberry, "A cross-sectional investigation of the suicidal spectrum: Typologies of suicidality based on ambivalence about living and dying," *Comprehensive Psychiatry,* vol. 53, pp. 461-467, 2012.

[25] J. J. Mazza and W. M. Reynolds, "Exposure to Violence in Young Inner-City Adolescents: Relationships With Suicidal Ideation, Depression, and PTSD Symptomatology," *Journal of Abnormal Child Psychology,* vol. 27, no. 3, pp. 203-213, 1999.

[26] R. Kessler, "Behavioral-Based Predictors of Workplace Violence in the Army STARRS," U.S. Army Medical Research and Materiel Command, Fort Detrick, 2014.

[27] P. Davis, "Primer for Building Factor Trees to Represent Social Science Knowledge," in *Proceedings of the 2011 Winter Simulation Conference*, Savannah, 2011.

Carrie Gardner is a Cyber Security Engineer with the Enterprise Threat & Vulnerability team in the CERT Division of the Carnegie Mellon Software Engineering Institute.

Ms. Gardner designs, develops, and transitions tools, algorithms, and exercises that enhance the ability of organizations to detect, prevent, and respond to insider threats. She specializes in data collection and analysis techniques, and empirical research methods.

Ms. Gardner holds a MS degree in Information Science from the University of Pittsburgh were she specialized in Cybersecurity and Data Analytics. Additionally, Ms. Gardner has completed a graduate certificate in Intelligence and International Affairs, a BA in Political Science, and a BA in Psychology. She formerly interned as an Intelligence Analyst with the Department of Homeland Security, and utilizes her background in intelligence analysis and threat assessment to aid her work in developing technical controls for measuring socio-technical indicators.

Ms. Gardner is also an Adjunct Faculty member of the University of Pittsburgh School of Computing and Information, where she teaches a course in Information Security Management.

Tracy Cassidy is an Insider Threat Researcher at the CERT Division National Insider Threat Center (NITC) of the Carnegie Mellon University Software Engineering Institute.

Ms. Cassidy leads research addressing the behavioral aspects of insider threat including targeted violence, suicidality, and radicalization. She has conducted research on national security espionage, unintentional insider threats, and positive incentives for mitigating insider threat.

Ms. Cassidy holds a M.A. in Clinical Psychology from New College of California and completed a four year intensive psychology internship working with issues of psychological trauma. She has a B.S. in Psychology and a minor in Sociology from the University of Pittsburgh. Ms. Cassidy has over 14 years of experience working in the mental health and substance abuse fields and was a practicing psychotherapist for many years. She also ran a program for the Department of Justice’s U.S. Probation and Pretrial Services and U.S. Bureau of Prisons for Northern California, Hawaii, and Guam providing clients entering and exiting federal prison with mental health and/or substance abuse treatment services.

Ms. Cassidy is a Chapter Development Chair for and a Board Member on the Washington DC Chapter of the Association of Threat Assessment Professionals (ATAP).