Lara Bagwell
ED520
Policy Proposal Plan

Summary:

The COVID-19 pandemic has accelerated the shift to permanent telework across the U.S. workforce, necessitating a new framework for how companies conduct risk management. While many workplaces are increasingly remote-friendly, most organizations still use tools and techniques designed for an office-only environment. Toriello-Fite argues that perimeter-based solutions that focus on defending from the outside are no longer enough; to succeed, Insider Threat programs and professionals must add technical and non-technical solutions that look at individuals and their behavior to provide context and to protect against data loss, system misuse, unauthorized disclosure of classified information, or kinetic violence from insiders. She provides a set of recommendations and resources to better mitigate risk in a remote work environment through increased training and education, the use of virtual applications and desktops (VDIs), strengthened coordination between communications, security, and human resources teams, and the use of User Behavior Analytics (UBA).

Policy Proposal Plan

Current Insider Threat programs (InTPs) and policies do not adequately address mental health conditions as precursors to insider threats. One Subject Matter Expert (SME) suggests in an interview with Code42 that "in 97% of the cases the insider was already under formal management and HR attention for concerning behaviors" (Code 42, 2020). Numerous recent examples across the Department of Defense (DOD), such as the 2019 murder/suicide shooting of three individuals in Pearl Harbor, HI, are subject to extensive investigations which reveal that mental health played some, if not a major role in the individual's actions (Harkins, 2020). Current DOD programs employ a range of screening measures, dependent on the individual's affiliation and status, from continuous vetting to randomized screening for illicit drug use. However, these programs do not go far enough to detect mental health concerns in individuals.

This paper will focus on the largest branch of the DOD, the United States Army, for the purpose of identifying specific policy gaps and recommending mitigation via an implementation plan.

I – Current Policy Gaps

There is some consensus amongst mental health experts regarding what kinds of mental health conditions pose a higher risk for insider threat. As general principles, employee depression, workplace or personal stress, and organizational conflicts/disagreements may contribute to individual insider threat risk (ObserveIT, 2017). More specifically, a 2009 study which utilized senor intelligence community adjudicators found that three personality disorders: psychopathy, malignant narcissism, and borderline personality organization associated with the highest level of insider threat risk (PERSEREC, 2011). A later DOD Personnel Security Research Center (PERSEREC) study argued that there are three categories of mental health issues that are of concern regarding insider threat: "(1) personality traits, (2) emotional issues and social skills deficits, (3) mental health symptoms and diagnoses" (PERSEREC, 2019, pp.5). The study also suggests that there is also a higher risk from individuals exhibiting "Dark Triad" personality traits. The "Dark Triad" is commonly understood as the combination of narcissism, Machiavellianism, and subclinical psychopathy (Kaufman et al., 2019). The concept of the "Dark Triad" is a modern one, originating in research in 2002, and becoming more widely studied in 2014-present (Kaufman et.al., 2019) and facilitating scientific understanding of the darker side of human nature. This information provides a means of identifying the specific kinds of mental health concerns relevant to insider threat, which provides a more specific framework to assist in identifying potential policy gaps.

A review of DOD Insider Threat policy, such as the National Insider Threat Policy and Minimum Standards reveals that at the federal and DOD level, there are broad requirements in place specific to mental health. Regarding the National Insider Threat Policy and Minimum Standards, the General Responsibilities set forth requirements for monitoring to include “personnel security information,” a centralized analysis/reporting/response capability, and information sharing across the organization (The White House, 2012, pp.1). DOD Directive 5205.16 specifically mentions mental health regarding the multi-disciplinary threat management capability that “includes the ability to share…mental health…information with commanders Component-wide” (Department of Defense, 2014, pp.13). Mental health is also mentioned as one of the areas where “subject matter expertise and multi-disciplinary capabilities are readily available to all commanders” (Department of Defense, 2014, pp.13). These higher-level policies provide ample room for subordinate components to build out their own programs and related requirements.

Focusing on the U.S. Army and its procedures, to attempt to identify potential gaps, personnel security personnel are responsible for conducting vetting of individuals in cleared or other special populations within the DOD. Vetting is conducted through the investigation process (SF86 completion, Subject interview and other investigative work), reporting of derogatory information when appropriate, and new continuous vetting conducted by the DOD Continuous Evaluation Program (DNI, 2018). In many cases, the personnel security process is the primary way mental health information of concern is identified. The SF86 asks several questions regarding mental health, specifically: 21A) Has the individual been the subject of an order declaring them mentally incompetent? 21B) Has a court or agency ordered the individual to consult with a mental health professional? 21C) Has the individual been hospitalized for a mental health condition? 21D) Has the individual ever been diagnosed with a list of mental health diagnoses? 21E) Does the individual have a mental health condition that "substantially adversely" affects their judgment, reliability, or trustworthiness, even if no current symptoms (OPM, 2016)? While thorough, these questions function based on the assumption that the individual will answer honestly and be forthcoming with relevant information. As already established, the spectrum of mental health issues that may lead to insider threat risk is broad, and in some cases, the concerns may remain subclinical and the individual is able to function somewhat normally in their position. Due to these issues, the SF86 questions alone are insufficient mitigation.

Looking further into the personnel security process, derogatory information is also identified through incident reporting, the individual self-reporting, or the responsible command initiating the action. These incident reports are based on the Adjudicative Guidelines, which are a set of standards used by DOD adjudicators to assess an individual's judgment, reliability, and trustworthiness in terms of accessing classified or sensitive information (DNI, 2017). If an individual has not sought treatment, or exhibited behaviors that have been documented (such as through commission of a crime or mental health hospitalization), the adjudicative guideline relies on self-reporting of disqualifying behaviors. This is again problematic as the kinds of individuals who may pose the greatest risk (such as subclinical psychopaths) are also not likely to self-report their disqualifying mental health status due to a documented tendency to also be pathological liars (Manson, J. et al., 2014).

As the final portion of the PERSEC process, the DOD Continuous Evaluation (CE) Program (which includes the U.S. Army's cleared populations) performs a frequent and randomized screening of individuals' Government and commercial records to identify unreported derogatory information (DNI, 2018). Due to its nature, CE can only detect mental health concerns when they manifest in a documentable way, such as the issuance of a Protection Order, commission of criminal conduct, financial issues, or other behavior that would present a trigger as "unreported derogatory information."

Looking beyond typical PERSEC mechanisms to detect mental health concerns potentially indicative of insider threat, two more areas are identified: mental health screening and treatment, and employee training and education. First, Army mental health screening and treatment is rigorous for Army military members and includes participation in a digital Periodic Health Assessment (PHA), data reporting to Commanders focusing on risk-reduction and suicide, and promotion of healthy behavior to include suicide prevention, stress management, and resiliency (U.S. Army, 2015, pp.18). These programs provide multiple opportunities for the Soldier to ask for help or to identify through health concerns that they are in need of mental health treatment. Most Army installations feature on-site Behavioral Health clinics that can provide a range of services from assessment and counseling to in-patient hospitalization and follow-up. These programs appear generally adequate for the Army military population, but not for the Army civilian and contractor populations.

The Army conducts Suicide Prevention Training for Active Army Soldiers, National Guard, Reserves, and Army Civilians as a regulatory requirement (U.S. Army, 2015, pp. 20). There are other required training areas, such as resiliency, specifically for the military population. Mental health reporting requirements are reiterated in Annual Security Refresher training for the same populations, as well as other security "touch-points" throughout one's career, such as Sensitive Compartmented Information (SCI) or Special Access Program (SAP) indoctrination, and other security training mandated by the Commander. However, these requirements do not afford an anonymous way to self-report or ask for help, nor do they provide ample coverage for the non-military populations. Army civilians have access to the Employee Assistance Program (EAP), but the program is somewhat narrow in scope, and in most cases results in a referral for training, assistance, or treatment with a third party provider. Additionally, use of the EAP necessitates the individual using their sick leave, annual leave, or pre- or post-duty hours for the service, just like they would for mental health coaching or counseling (Fort Carson EAP, 2021).

II – Qualification of the Critical Path Model

The behavioral model known as the "Critical-Path Method" provides an excellent tool for evaluating mental health concerns as a potential indication of increased insider threat risk. The model utilizes four elements to "describe the personal predispositions that have contributed to individuals committing acts against their organizations (Shaw & Sellers, 2015, pp.2)." In other words, this model focuses heavily on an individual's behavior to try and predict a path to a hostile act, as a general risk assessment tool. To do this, the Critical-Path Method uses four elements: Personal Predispositions, Stressors, Concerning Behaviors, and Problematic Organizational Responses, and the accumulation/cumulative effect of these factors over time to predict an individual's likelihood to commit a hostile act.

A 2015 paper by Sellers & Shaw overlays the Critical-Path Method with numerous historical insider threat examples such as Chelsea Manning, Ana Montes, Jonathan Pollard, and Thomas Dolce to prove its accuracy and usefulness (Sellers & Shaw, 2015, pp. 4). A great strength of the model is its recognition of the importance of mental health concerns that might fly under the radar and are therefore under-reported (such as "kooky" behavior of Pollard or Montes alienating her colleagues) (Sellers & Shaw, 2015, pp.5). Most importantly, for the purpose of this paper, the final element, or Problematic Organizational Responses, accounts for potential areas of gaps or inattentiveness on behalf of management that may indicate the insider threat risk is higher. This tool is extremely useful, simplistic enough to enable rapid implementation, and highly recommended for the Army's use as potential improvements to mental health concern detection and mitigation are evaluated (such as the three recommendations which follow).

III – Implementation Plan

Based on the discussions of Army mental health policy and programs and related insider threat considerations, this implementation plan contains three recommendations specific to mental health that allow for specific areas of change and policy revision rather than a general overhaul of programs.

The first recommendation is implementing supplemental annual psychological screening for certain Army populations, both military and civilians (those in cleared and/or Arms, Ammunition, and Explosives or AA&E positions). Current requirements chiefly pertain to Army military populations. If an individual does not indicate voluntarily that they need psychological screening through a Health Assessment, commit an act of concern (such as a crime or violent outburst at work), or require supplemental screening for a new duty assignment, they may never have the opportunity to speak with a mental health provider or indicate they need treatment. Implementation is recommended in conjunction with existing Army digital training, specifically the Annual Security Refresher. It is recommended that a series of questions, including "would you like to speak to an Army provider regarding your mental health?" be provided at the end of the training.

If the individual answers in the affirmative, their information is sent, in accordance with all applicable privacy laws, to the correct provider based on their affiliation (IE: EAP for an Army Civilian) for evaluation and action. If this version of digitally asking the individual if they need help is proven insufficient, a more drastic version requiring significant manpower and resources is needed. For instance, requiring the same group of individuals to attend an annual appointment screening with an Army provider. This appointment could consist of assessment tools and a discussion with the provider to ascertain the individual's current mental health state and whether or not they are in need of additional resources. A 2019 PERSEREC study recommends that "screening should focus first on individuals who present the highest risk due to job position and DoD should further triage based on the results of an assessment process to identify even smaller groups of individuals for more extensive psychological evaluation" (PERSEREC, 2019, pp.7). Conception and implementation of any version of these requirements should only occur after significant coordination with Army mental health SMEs. The final portion of the process must require that if derogatory information that falls within the Adjudicative Guidelines is identified, it must be reported in the security system of record by the responsible Security Manager in accordance with established procedures that do not constitute privacy concerns.

The next recommendation is requiring additional mental health training for individuals in management/supervisory positions, particularly the civilian population. Current training requirements for these individuals mirror the training requirements already discussed in this paper, but may add additional courses (such as EEO) from the supervisor's optic, and/or courses regarding supervisory actions such as timecards or employee discipline. The recommendation is to stand up a new training program consisting of in-person quality mental health training focused on employee well-being, potential indicators of trouble, and de-escalation techniques. A recent study from Lancet Psychiatry found that giving managers "just four hours of training on mental health" resulted in an 18% reduction in work-related sick-time off (compared to a 10% rate in a control group) (ObseveIT, 2018). This training should be designed and conducted by Army mental health professionals. As a 2018 PERSEREC study found, "insider threat behavior takes place in a social context, and environmental factors can both facilitate and mitigate individual decisions" (PERSEREC, 2018, pp. 16). It is extremely difficult for supervisory personnel within Army organizations to influence environmental factors that may have a positive effect on individuals (such as incident response, or supporting a high trust organization) without adequate training. Finally, de-escalation training provides the supervisor with the skills to prevent potentially volatile situations from unnecessarily exacerbating by empowering them with communication skills comparable to those utilized by mental health and law enforcement professionals.

Finally, as previously discussed, changes over time in certain aspects of behavior (such as language use) are highly linked to potential insider threat risk. The Army, and greater Federal Government, has excellent tools at its disposal to attempt to analyze behavioral change in employees. Specifically, language use across Government communication platforms, considering the Army already possesses monitoring capabilities for network e-mail, as well as instant messaging through programs such as MS Teams or Skype for Business. A DOD study regarding Psychological Content Analysis in written communications found that frequent references to victimization vocabulary was a potential indication of an individual at risk (Stroz et al., 2017). Applying software solutions to conquer this kind of analytical problem allows for a less invasive approach and a more objective treatment of the data (as the software is the one doing the search over time). Similarly to the other recommendations, if an individual of concern is identified based on problematic changes in language, the material should be reviewed by a mental health professional who can speak further with the individual before determining whether or not the issue is reportable. DOD InTPs already must contain some level of user monitoring as a minimum standard (Department of Defense, 2014), and adding Psychological Content Analysis to this user monitoring would be cost-effective. All recommendations levied by this paper assume the Army is open to the potential additional manpower requirement posed by changes or additions to mental health screening (such as Content Analysis) or training. Further, all three recommendations must be first supported by revised Army policy to ensure ease and efficiency of implementation.

IV – Conclusion

In conclusion, adequately mitigating insider threat risk related to mental health concerns is a daunting task for any large organization. Recent insider threat incidents ranging from kinetic violence to espionage support the need for better mental health screens, and to train individuals on how to better mitigate concerns. The three recommended changes outlined in this paper provide senior officials with an implementation plan that will likely result in significant positive change across the Army. As future insider threat incidents occur, they must be thoroughly studied to determine lessons learned and whether or not additional changes are needed in the area of mental health. If the Army can adopt a more proactive posture with improved mental health screening (both of the individual and their communications) and training for certain populations, future insider threat risks may be successfully mitigated.

References

Code 42 (2020). Expert Q&A: The Psychology Behind an Insider. https://www.code42.com/blog/expert-qa-the-psychology-behind-an-insider/.

Department of Defense. (2014). The DoD Insider Threat Program, Directive 5205.16. https://www.cdse.edu/documents/toolkits-insider/dod-dir-5205-16-sep-30-2014.pdf.

Fort Carson EAP (Accessed April 20, 2021). Employee Assistance Program. https://www.carson.army.mil/assets/docs/dhr/eap-brochure.pdf.

Harkins, Gina. (2020, September 29). Sailor Behind Pearl Harbor Shooting was ‘Insider Threat’ with Underdiagnosed Mental Issues. Military.com. https://www.military.com/daily-news/2020/09/29/sailor-behind-pearl-harbor-shooting-was-insider-threat-underdiagnosed-mental-issues.html.

Kaufman, Scott., Yaden, Bryce., Hyde, Elizabeth., Tsukayama, E. (2019, March 12). The Light vs. Dark Triad of Personality: Contrasting Two Very Different Profiles of Human Nature. *Frontiers in Psychology*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6423069/.

Manson, J., Gervais, M., Fessler, D., Kline, M. (2014, November 26). Subclinical Primary Psychopathy, but not Physical Formidability or Attractiveness, Predicts Conversational Dominance in a Zero-Acquaintance Situation. *PLOS One.* https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0113135.

ObserveIT. (2018, September 7). Could Mental Health Coaching Be the Secret to Insider Threat Prevention? ObserveIT. https://www.observeit.com/blog/could-mental-health-coaching-be-the-secret-to-insider-threat-prevention/.

PERSEREC. (2011). Identifying Personality Disorders that are Security Risks; Field Test Results, PERSEREC TR 11-05. https://www.dhra.mil/Portals/52/Documents/perserec/tr11-05.pdf.

PERSEREC. (2018). A Strategic Plan to Leverage the Social & Behavioral Sciences to Counter the Insider Threat, PERSEREC-TR-18-16. https://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-18-16-Strategic-Plan.pdf.

PERSEREC. (2019). An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks, PERSEREC-TR-19-05. https://www.dhra.mil/PERSEREC/Selected-Reports/#TR19-05.

DNI. (2017, June 8). Security Executive Agent Directive 4, National Security Adjudicative Guidelines. https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf.

DNI. (2018, January 12). Security Executive Agent Directive 6, Continuous Evaluation. https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf.

OPM (2016, November). Questionnaire for National Security Positions. https://www.opm.gov/forms/pdf_fill/sf86.pdf.

Shaw, E., and Sellers, L. (2015). Application of the Critical-Path Method to Evaluate Insider Risks. CIA. https://nationalinsiderthreatsig.org/itrmresources/Application%20Of%20The%20Critical-Path%20Method%20To%20Evaluate%20Insider%20Risks-June%202015.pdf.

Stroz, E., Weber, S., & Shaw, E. (2017, April 24). Psychology is the key to detecting internal cyberthreats. Retrieved April 14, 2021, from https://hbr.org/2016/09/psychology-is-the-key-to-detecting-internal-cyberthreats.

The White House. (2012). National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy__Minimum_Standards.pdf.

US Army. (2015, April). Army Health Promotion, Army Regulation 600-63. https://www.army.mil/e2/downloads/rv7/r2/policydocs/r600_63.pdf.