UNIVERSITY OF MARYLAND

7005 52nd Avenue
College Park, Maryland 20742

A National Research Agenda on Insider Threat

Petra Bradley,[1] Wendy Chambers,[1] Cory Davenport,[2] & Lelyn Saner[1]

[1]University of Maryland, Center for Advanced Study of Language (CASL)
[2]National Consortium for the Study of Terrorism and Responses to Terrorism (START)

1. How are insider threats impacting national security?

Insiders cause harm by leveraging their knowledge of and access to an organization to commit a crime (Gelles, 2016) such as a violent attack (e.g., Ft. Hood, Texas in 2009 and the Naval Yard in Washington D.C. in 2013), or by leaking sensitive government information (e.g., Edward Snowden in 2013 and Reality Winner in 2017). Insider incidents such as these can cost lives and often cause fear in both the affected workforce and the community, but they are also relatively rare. Other insiders pose security risks by sabotaging government projects, and still others pose a threat through indirect means, i.e., by being careless or inattentive to their duties. Any of these types of insider threat may impact national security by compromising intelligence sources and methods, by distributing classified or sensitive information, by disrupting operations, or by destroying government assets in the form of both property and lives.

2. Social and Behavioral Science research critical to this survey

2.1. Existing research: Identifying risk factors for workplace violence (Kausch & Resnick, 2001) or other types of insider threat is not new; the challenge is how to define and measure these factors, prevent threatening behaviors, and create the most effective threat detection and prevention strategy for individual organizations and environments. For example, Gelles, as well as others (Intelligence and National Security Alliance, 2017; Shaw, Ruby, & Post, 1998), identify not only traits associated with insider threat but also the role played by others in the work environment who unwittingly overlook the red flags of the insider (Gelles, 2016) and in some cases may even provoke behavior (Neuman & Baron, 1998). In other words, prevention should not focus solely on the perpetrator of an incident. Here we review some of the research focused on predicting insider threat and what motivates insiders, and look to literatures that may be useful in helping to understand how to increase reporting behavior and improve reporting culture within organizations.

Much of the associated research and models used to predict insider threat focus on information technology (IT) both in terms of vulnerability and behavior (Chinchani, Iyer, Ngo, & Upadhyaya, 2005; Kandias, Mylonas, Virvilis, Theoharidou, & Gritzalis, 2010; Magklaras & Furnell, 2001). Even though insiders who pose a threat via IT systems may overlap with other types of threats in terms of motivation, it is difficult to assess motivation of behavior observed on an IT system. A simple mistake can appear malicious, and vice versa. Some studies of IT “threat” substitute types of behaviors that might be considered mundane misuse of IT resources (Magklaras & Furnell, 2001), rather than more large-scale threats to the organization. True threat behavior is relatively rare, making it difficult to research, but it is also unlikely that mundane misuse is motivated by the same factors that motivate threat. Misuse of resources can be viewed as a continuum, and most who commit mundane misuse will not go on to pose a larger threat, though those who do pose an insider threat may start as mundane misusers. For example, someone who breaks a minor physical security rule, such as bringing a knife longer than the regulation four inches to cut an apple most likely poses no threat, but in rare instances they may be an individual testing the threshold of enforcement of the rules.

Some research addresses motivations of actors and context that may have influenced them, and to a lesser extent the behavioral and cognitive attributes of individuals who have posed threats in the past. Motivating factors include a false sense of entitlement, personal or social frustrations, ethical flexibility, reduced loyalty to the organization, and lack of empathy (Shaw, Ruby, & Post, 1998). Lack of empathy, in particular, is listed among a collection of traits in psychopathy (Hare, 1991; Kahn, Byrd, & Pardini, 2013). Some psychopaths are described as cold, calculating (Dean et al., 2013), yet superficially charming, sometimes referred to as corporate psychopaths (Akhtar, Ahmetoglu, & Chamorro-Premuzic, 2013), and are possibly associated with white-collar crime (Ray, & Jones, 2011). Key researchers in the field argue that psychopathy might be more prevalent in the workplace than in the general populace, perhaps by as much as 10% (Bracken, 2007). It might therefore be useful to use an instrument for measuring psychopathy, given that psychopathy includes several traits identified in insider studies.

Many insiders developed their intention to act after they were in the job, so while it is important to detect who is vulnerable to becoming a threat at the point of hiring, it will likely need to be complemented by periodic monitoring (e.g., as part of periodic assessments required to retain a clearance) for triggering events such as loss of social support (e.g., via estrangement from family or friends or death of a loved one, especially by suicide) that may be associated with an increased incidence of violent behavior (Barling, 1996). However, there are currently no recommendations as to how often to appraise such factors, nor the best way to do so, given that some emotional shift would be normal and expected after a loss. Monitoring employees is potentially low-tech and low-overhead but would likely require reporting via supervisors or encouraging anonymous peer-reporting. Any system of monitoring will need to balance privacy needs and the impact on employee morale with safety concerns.

Other areas that may shed light on the issue of detecting insider threat include research on deception detection, violence in schools, and domestic violence. With regard to who is likely to report threat behavior, research on whistleblowing[1] may provide insights about the personal traits and situational characteristics associated with reporting behavior in a work context (Ahern & McDonald, 2002), and bystander behavior research may help us understand when people choose action over inaction (Banyard, 2008), whether due to personal (e.g., Baumert, Halmburger, & Schmitt, 2013) or situational variables (e.g., Miceli & Near, 1988).

2.2. Recent advances: Most tools applied to any problem today involve data analytics, and insider threat is no exception. Novel means of identifying insider threats in the workplace have emerged in recent years, such as biometric assessments and linguistic analysis to reveal deception or trust. The experiments on detection of variation in pulse, temperature, and skin conductivity to reflect emotions associated with threat behaviors have indicated some confirmatory relationships (Gamer, Bauermann, Stoeter, & Vossel, 2007). However, this approach may be impractical for most organizations, given the low likelihood of employees consenting to even mildly invasive technology, the increased likelihood of false positives due to a variety of individual and environmental factors, and the equipment and analytical overhead involved (Lee, Park, Eom, & Chung, 2015). Linguistic analysis of internal communications offers promise as a tool in assessing risk of insider threat (Ho et al., 2016). A comparatively more feasible method might be to apply the Linguistic Inquiry and Word Count (LIWC) text analysis program to assess whether individuals committing insider threat behaviors change their word usage to be more self-focused (e.g., I versus we), and to decrease linguistic mimicry in emails (Taylor, et al, 2013).

Some research has shifted away from identifying individuals who are an increased risk of posing a threat to focus on identifying vulnerabilities within an organization. Researchers at the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START) have developed a tool designed to characterize the deterrent value of existing safety, security, regulatory, and business systems and identify where enhancements are needed to reduce insider threats (Abugo, 2015).

3. Central questions

We propose that a program of research on insider threat should take a holistic approach that focuses on the following areas:

[1] This term was originally intended to describe the "whistleblower" as the individual who reports mis-deeds, hostile work environments, or unsafe practices. The term has become politically-charged, however, as some incidents have caused the whistleblower him- or herself to be seen as disloyal to the organization. Additionally, "whistleblower" has been used to describe people such as Edward Snowden, who might be seen by some as "blowing the whistle" on government over-reach, but more traditionally would have been viewed as the one posing the insider threat. For this reason, we use the term "threat reporter."

3.1. Insiders

3.1.1. Are there cognitive, personality, or other factors associated with individuals who may become an insider threat that can be detected prior to hiring?

3.1.2. Are there warning signs (e.g., increased cognitive load, deception) that can be detected using periodic screening methods to determine which current employees are at an increased situational risk for posing a threat?

Although some factors are currently assessed in both industry and government, most protocols assess only a small number of factors and in many cases these are not factors that have been validated as being associated with risk of threat. Moreover, while some government agencies conduct periodic assessment (e.g., as part of the clearance process), industry employees are rarely assessed in this way after the point of hire. New research should build on existing models of insider threat such as those developed by the Intelligence and National Security Alliance (2017) to focus on what can be assessed, the best measures for doing so, and the intervals that best position the agency to detect a threat prior to an incident. In particular, it will be critical to develop tools for monitoring and methods to determine what combinations of life stressors and individual traits lead to individuals posing a threat to their organization.

3.2. Threat Reporters

3.2.1. Are there cognitive, personality, or other factors associated with individuals who are most likely to *report* signs that colleagues may pose an insider threat? If so, can we select for these factors when hiring in certain high-risk career fields?

3.2.2. Are there behaviors of threat reporters that can be taught to others? Can we train or incentivize people to report who would otherwise be unlikely to take action?

3.3. Organizational Culture

3.3.1. Can organizational vulnerabilities be identified?
START's model focuses on air cargo transport, but with additional research it could be adapted to other contexts. This area of research would allow detection of individuals as well as additional surveillance and prevention measures to be focused in the areas of greatest vulnerability.

3.3.2. What features of organizational culture are associated with elevated risk, and can organizations be adapted to reduce risk of threat and increase the likelihood that troubled employees can be helped without compromising privacy? Are there organizational structures, leadership styles, or types of power structures that make insider threat more or less likely?

It will be critical to facilitate sharing of government and industry data with researchers to move toward systems of threat detection that consider a variety of indicators.

4. Benefits for advancing fundamental knowledge

It is critical to build a holistic theory to understand what causes someone to be an insider threat, both as an individual (e.g., cognitive factors and personality factors) and in terms of situational and organizational factors, as well as how best to detect such threats (e.g., empowering fellow employees to notice and report). With an improved understanding of these factors, we can build instruments to allow us to hire individuals who are less likely to pose an insider threat and to help us monitor individuals' likelihood of posing a threat during their tenure at the job. It will also allow cultivation of a more proactive reporting culture if we can select people who are more likely to provide information to the right individuals or identify behaviors that can be taught to people to improve appropriate reporting. Additionally, research into the features of the organization that bear on their risk of insider threat would allow the organization to take appropriate action to minimize vulnerabilities and to tailor new organizational structure to reduce the risk of threat. Strategies that make the process of granting clearances and internal investigation of personnel more efficient and effective would save money for both the government and industry and would both make our workplaces safer and reduce the chances of leaking of sensitive information.

References

Abugo, O. (2015, November). START team assesses insider threat for international air cargo. Retrieved from http://www.start.umd.edu/news/start-team-assesses-insider-threat-international-air-cargo

Ahern, K., & McDonald, S. (2002). The beliefs of nurses who were involved in a whistleblowing event. *Journal of Advanced Nursing*, *38*(3), 303-309.

Akhtar, R., Ahmetoglu, G., & Chamorro-Premuzic, T. (2013). Greed is good? Assessing the relationship between entrepreneurship and subclinical psychopathy. *Personality and Individual Differences*, *54*(3), 420-425.

Banyard, V. L. (2008). Measurement and correlates of prosocial bystander behavior: The case of interpersonal violence. *Violence and victims*, *23*(1), 83-97.

Barling, J. (1996). The prediction, experience, and consequences of workplace violence. *Violence on the job: Identifying risks and developing solutions*, *2949*.

Baumert, A., Halmburger, A., Schmitt, M. (2013). Interventions against norm violations: Dispositional determinants of self-reported and real moral courage. *Personality and Social Psychology Bulletin, 39*(8), 1053-1068.

Bracken, D. W. (2007). [Review of the book *Snakes in suits: When psychopaths go to work,* by P. Bibiak & R. D. Hare]. *Personnel Psychology, 60*, 257-260.

Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005, June). Towards a theory of insider threat assessment. In *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on* (pp. 108-117). IEEE.

Dean, A. C., Altstein, L. L., Berman, M. E., Constans, J. I., Sugar, C. A., & McCloskey, M. S. (2013). Secondary psychopathy, but not primary psychopathy, is associated with risky decision-making in noninstitutionalized young adults. *Personality and individual differences*, *54*(2), 272-277.

Hare, R. D. (1991). *The Hare psychopathy checklist-revised: Manual*. Multi-Health Systems, Incorporated.

Ho, S. M., Hancock, J. T., Booth, C., Burmester, M., Liu, X., & Timmarajus, S. S. (2016, January). Demystifying insider threat: Language-action cues in group dynamics. In *System Sciences (HICSS), 2016 49th Hawaii International Conference on* (pp. 2729-2738). IEEE.

Intelligence and National Security Alliance, Security Policy Reform Council, Insider Threat Subcommittee (2017, April). *Assessing the mind of the malicious insider: Using a behavioral model and data analytics to improve continuous evaluation.* Retrieved from: http://insa.informz.net/INSA/data/images/Docs/WhitePapers/INSA_WP_Mind_Insider_FIN.pdf

Gamer, M., Bauermann, T., Stoeter, P., & Vossel, G., (2007). Covariations among fMRI, skin conductance, and behavioral data during processing of concealed information. *Human Brain Mapping,* 1287- 1301.

Gelles, M. G. (2016). *Insider threat: Prevention, detection, mitigation, and deterrence.* Cambridge, MA: Elsevier.

Kahn, R. E., Byrd, A. L., & Pardini, D. A. (2013). Callous-unemotional traits robustly predict future criminal offending in young men. *Law and human behavior*, *37*(2), 87.

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., & Gritzalis, D. (2010, August). An insider threat prediction model. In *International Conference on Trust, Privacy and Security in Digital Business* (pp. 26-37). Springer Berlin Heidelberg.

Kausch, O. & Resnick, P. J. (2001). Assessment of employees for workplace violence. *Journal of forensic psychology practice*, *1*(4), 1-22.

Lee, H. J., Park, M. W., Eom, J. H., & Chung, T. M. (2015). New Approach for Detecting Leakage of Internal Information; Using Emotional Recognition Technology. *TIIS*, *9*(11), 4662-4679.

Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62-73.

Miceli, N.P. & Near, J.P. (1988). Individual and situational correlates of whistle blowing. *Personnel Psychology*, *41,* 267-281.

Neuman, J. H., & Baron, R. A. (1998). Workplace violence and workplace aggression: Evidence concerning specific forms, potential causes, and preferred targets. *Journal of management*, *24*(3), 391-419.

Ray, J. V., & Jones, S. (2011). Self-reported psychopathic traits and their relation to intentions to engage in environmental offending. *International Journal of Offender Therapy and Comparative Criminology*, *55*(3), 370-391.

Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, *2*(98), 1-10.

Taylor, P. J., Dando, C. J., Ormerod, T. C., Ball, L. J., Jenkins, M. C., Sandham, A., & Menacere, T. (2013). Detecting insider threats through language change. *Law and human behavior*, *37*, 267.