OPA PERSEREC
OFFICE OF PEOPLE ANALYTICS | PERSONNEL AND SECURITY RESEARCH CENTER

Insider Threat: Social Science Insights and Applications

Presented at the World Institute For Nuclear Security (WINS) Conference, December 16, 2018

Dr. Eric L. Lang, Director, PERSEREC

Personnel and Security Research Center (PERSEREC)
Office of People Analytics, U.S. Department of Defense

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the DoD, OPA, or PERSEREC

WHAT IS PERSEREC?

PERSEREC is a U.S. Department of Defense (DoD) research center dedicated, since 1986, to applying…

social science to improve the effectiveness, efficiency, and fairness of personnel security, insider threat, suitability, and reliability systems.

PERSEREC INSIDER THREAT RESEARCH AREAS RELEVANT TO IMPROVING POLICIES & TOOLS

- Emerging threats such as social media applications for personnel risk
- Contextual and organizational factors that interact with individual dispositional factors to exacerbate or mitigate risk
- Automated tailored Continuous Evaluation “CE” of personnel
- Definitions and metrics for security vetting and CE related quality, to advance assessments of policy and program effectiveness, and continuous improvement
- Assessing and managing mental health issues related to personnel security, suitability, insider threat, & self harm

INSIDER THREATS, MOTIVATIONS, & BEHAVIORS VARY

Insider Threat = Security and/or safety risks—intentional or unwitting—associated with trusted employees, military personnel, contractors or organizational partners

- **Government Espionage/Leaks**
  e.g., cleared employee provides classified info to a foreign group
- **Corporate Espionage**
  e.g., employee steals intellectual property for personal gain or to sell to a competitor
- **Terrorism/Violence**
  e.g., radicalized personnel turns violent
- **Vandalism/Disruption**
  e.g., vengeful employee harms the organization's computer system
- **Reliability Problems and Gross Negligence**
  e.g., employee with alcohol/substance abuse, psych problems, or gross incompetence fails to protect sensitive info/systems

Because motivations, behaviors and other influences vary across these risk areas, there is no single reliable and valid social science model for predicting insider threats

INSIDER THREAT PROBLEM: EXAMPLES & MAGNITUDE

- “Lone wolf” insiders vs insider/outsider collaborations vs negligent/unreliable insiders

- Nuclear facility sabotage, such as arson, by onsite employees and contractors has occurred at many facilities worldwide (including eight in the U.S.), with individual damage costs of millions of U.S. Dollars (USD) in addition to injury and risks to facility staff, the surrounding community, as well as ongoing fear and loss of confidence. Examples (From CRDFGlobal.org, 2017) include:

  - South Africa (1982): a Koeberg nuclear power station worker detonated four bombs at the facility in an act of resistance against apartheid
  - France (2012): a European Organization for Nuclear Research particle physicist offered help to an al-Qaida affiliate to carry out attacks
  - Belgium (2014): a Doel nuclear power plant employee forced a shutdown of the reactor after intentionally draining the lubricant for its turbine (resulted in more than100 million in repairs)

INSIDER THREAT PROBLEM: EXAMPLES & MAGNITUDE

- With respect to insider threat prevalence, risk of a terrorist incident is low but likely to increase in the future.
- Insider threat generally occurs in three varieties of decreasing frequency (ICIT, 2017):

1. Careless or uninformed insiders who **unintentionally violate security requirements** and policies due to a lack of cybersecurity awareness and training (“cyber-hygiene”).

2. Negligent insiders who **intentionally evade security measures** out of convenience, neglect, or misguided attempts to increase productivity.

3. Malicious insiders who **intentionally evade security measures** in attempts to profit financially, gain revenge, or seek to unmask corruption or other malfeasance, based on a misguided sense of idealism.

INSIDER THREAT PROBLEM: EXAMPLES & MAGNITUDE

- "Cyber crime damages [across all sources] will cost the world $6 Trillion (USD) annually by 2021, up from $3 trillion in 2015," and "is the greatest threat to every [organization] in the world." (2017 State of Cybercrime)

- Cyberattacks are more often perpetrated by insiders—by malice or negligence—than by external attackers.

- Among malicious intentional insider attacks:
  - 62% involved employees trying to establish a second income stream from their employer's sensitive data
  - 29% stole information as they exited employment for future financial gain
  - 9% were saboteurs

UNDERSTANDING INSIDER THREAT: TECHNOLOGICAL FACTORS ARE IMPORTANT, BUT HUMAN FACTORS ARE MORE IMPORTANT

- In most insider cases, reporting or follow-up behaviors were either too slow, uncoordinated, or wrong.

- How does someone become a risky insider?

  – **Dispositional factors (e.g., personality & mental health) interact over time with:**
    - Individual events and stressors
    - Organizational and contextual influences

  – **Need, network, narrative**: (A. Kruglanki’s radicalization model)

BEHAVIORAL INDICATORS OF POTENTIAL RISK

- Unwillingness to comply with rules and regulations or security requirements
- Signs of alcohol abuse, drug misuse or illegal drug use
- Apparent or suspected mental health issues
- Criminal conduct or affiliation with criminals, violent groups or online radicals
- Misuse of organizational property or systems, or inappropriate “work-arounds”
- Threatening language
- Serious lying, evasiveness, defensiveness, or inability to correct own bad behavior
- Serious disloyalty or disinterest in the mission/needs of the organization or nation
- Attempts to access files or facilities not clearly within their work responsibilities
- A pattern of counterproductive work behaviors
- Unexplained affluence

And, generally:

- Any behavior that raises doubts of continued reliability or safety, such as sudden uncharacteristic behavioral changes, rage, recklessness or disconcerting and rigid preoccupations (especially regarding weapons or violence)

INDICATOR LISTS ARE CRITICAL BUT LIMITED

- Successful insider threat management relies on timely and proper follow-up and coordination after a potential (likely ambiguous) concern has been identified.

- Many identified personnel will be properly addressed through Human Resources (HR) support rather than by security or counterintelligence intervention (e.g., due to alcohol, drug, stress, or mental health issues).

INSIDER THREAT SCIENCE-BASED INSIGHTS & BEST PRACTICES

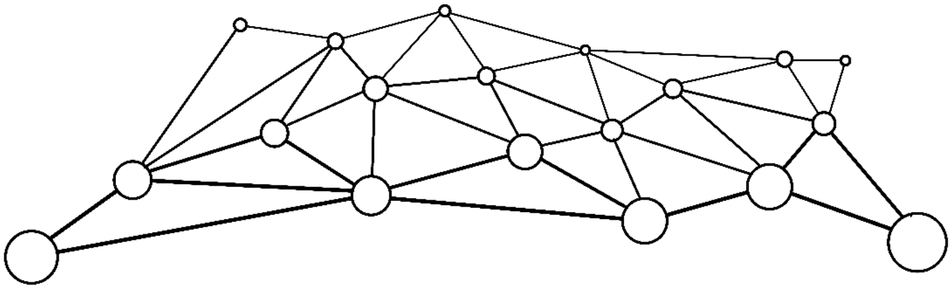
1. Initial personnel screening is critical but not sufficient. Continuous Evaluation "CE" (tailored for risk management) is more important.

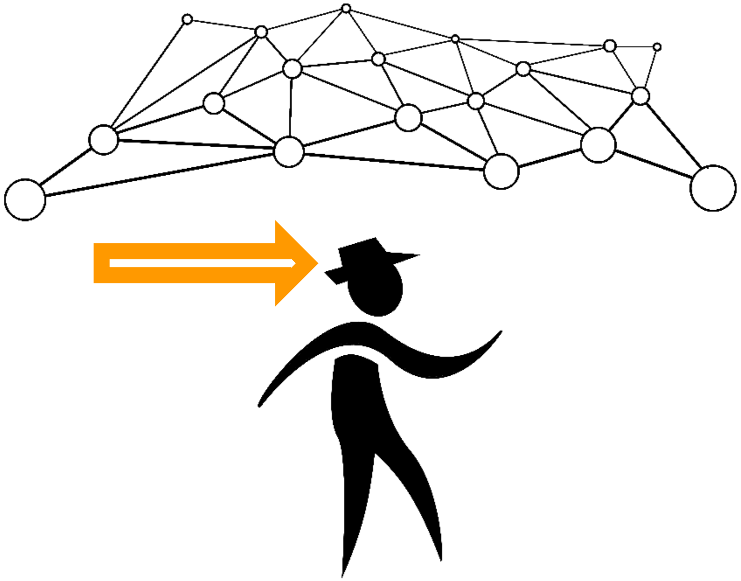
2. Organizations need to better develop and communicate to employees a healthy and effective atmosphere of the need for Insider Threat programs, individual's roles and how programs will be conducted fairly. Listen to and discuss employee concerns and questions. (e.g., 2018: 70% employees would quit if covert monitoring was found)

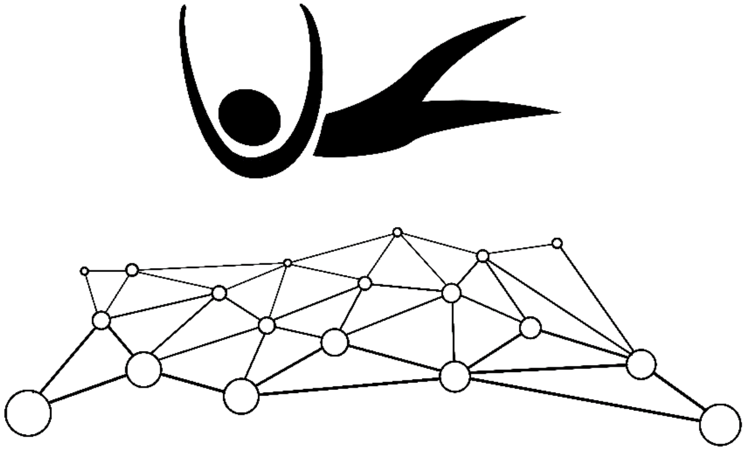
3. Organizations need to better understand office climates and cultures (e.g., levels of frustration, unfairness, toxic leadership, tolerance for rule-breaking, trust) and how these contexts exacerbate or mitigate Insider Risks. Most bad and good behaviors result from interactions of individual's dispositions and environmental factors.

4. Need to integrate info from many relevant and privacy-appropriate sources, e.g., criminal, financial, travel (and other databases), network user activity monitoring, supervisor/coworker reporting, social media; assessed by an Insider Threat hub (i.e., an integrated NET for "Neutralizing Enterprise Threat"). Most important, Security and Human Resource personnel must work together, and both should be represented in an organization's insider threat integration hub.

WHY THE “NET” METAPHOR?







INSIDER THREAT SCIENCE-BASED INSIGHTS & BEST PRACTICES

5. Most mental health issues are not insider threat issues. Need to define the narrow set of mental health issues of concern, reduce mental health stigma and promote mental health treatment, which will improve overall workplace health, productivity, trust and organizational culture and, consequently, reduce employee frustrations that can exacerbate some types of insider risk.

6. Improve the definitions and metrics of insider threat program quality and effectiveness. Go beyond reliance on implementation compliance and employee self reported satisfaction. Need more emphasis on what constitutes effective training.

   - Employ interactive didactic insider case group discussions, pausing often throughout the case timeline to ask participants “at this point, who knows what? What could or should be done? What are the risks and ethics of different options?”

7. Improving supervisor/coworker reporting is the biggest underutilized source of helpful info to mitigate Insider Threats. However, reporting ("snitching“) is psychologically challenging, and many "see something, say something" trainings are typically weak.

BARRIERS TO COWORKER AND SUPERVISOR REPORTING

- Social science research identifies psychological barriers to reporting
  - Socialization and cultural norms: “don’t be a snitch”
  - Expectations of peer loyalty: “code of silence”
  - Concerns about the outcome: “I don’t want coworker to lose his job”
  - Fear of retaliation

- Organizationally, reporting processes are not always well understood
  - What to report?
  - How to report (to whom)?
  - What will happen after a report is made?

OVERCOMING BARRIERS TO REPORTING

- Establish a clearly defined reporting process
- Make the outcome of the process transparent
- Increase felt responsibility and mutual responsibility
- Make the process non-punitive
- Eliminate risks associated with disclosure
- Train and test employee understanding and ability
- Emphasize the positive aspects of reporting
  - Preventing a larger problem or safety risk to others
  - Facilitating help or support for a struggling coworker

TRAINING AND ASSESSMENT RESOURCES

- U.S. Center for Development of Security Excellence (CDSE) Insider Threat training videos, toolkits and documents. Many are open-source and freely available at: https://www.cdse.edu/index.html
- CERT's 2016 (5th edition), "Common Sense Guide to Mitigating Insider Threats," freely available at: https://resources.sei.cmu.edu/library/
- Institute for Critical Infrastructure Technology (ICIT) Feb 23, 2017, paper "The Insider Threat Epidemic Begins," freely available at: http://icitech.org/event/icit-monthly-briefing-insider-threat/ or by request from: https://icitech.org/
- M. Bunn and S. Sagan's 2017 book "Insider Threats," which includes helpful analyses of relevant insider threat case studies
- PERSEREC research and tool for assessing risky personality disorders using "Dispositional Indicators of Risk Exposure" DIRE

SUMMING UP; FOUR MAIN TAKE-AWAY POINTS

1. Excellent technology, policies and staff are necessary but not sufficient to "Neutralize the Enterprise Threat" of risky insiders. Integration of information and coordinated follow-up among organizational components—especially security and HR—are the keys to effectiveness.

2. Your employees and management staff will be the most important determinants of an effective approach, as well as its greatest weakness. Threat management successes and failures are most often due to social-psychological factors (not technology, policy, locks or indicator lists).

3. Have open and meaningful discussions with employees about personnel and organizational security needs, their concerns, rights and responsibilities, and what they can expect from the organization.

4. Employ engaging training methods and improve measures of effectiveness.

MORE INFORMATION AND CONTACT

Selected reports, products and additional information are available on our website:

http://www.dhra.mil/perserec/

or by contacting:

Dr. Eric L. Lang (Director, PERSEREC)

Eric.L.Lang6.civ@mail.mil

perserec@mail.mil

ADDITIONAL & BACKUP MATERIAL

- Data Science predictive models (e.g., machine learning, “Big Data” and AI algorithms) provide important and powerful analytic tools but must be combined with social science substantive knowledge to avoid producing fast and powerful, biased, unhelpful and unethical results (e.g., “Weapons of Math Destruction” and “Frankenalgorithms”).

- The importance of fostering “Psychological Safety” in your workplace. Google Spent 2 Years Studying 180 Teams. The Most Successful Ones Shared 5 Traits; for more:
  - https://rework.withgoogle.com/guides/understanding-team-effectiveness/steps/foster-psychological-safety/
  - https://www.nytimes.com/2016/02/28/magazine/what-google-learned-from-its-quest-to-build-the-perfect-team.html
  - https://www.inc.com/michael-schneider/google-thought-they-knew-how-to-create-the-perfect.html