OPA
OFFICE OF PEOPLE ANALYTICS

PERSEREC
PERSONNEL AND SECURITY RESEARCH CENTER

Science-based Insights for Understanding & Mitigating Insider Threats

Presented at the World Institute for Nuclear Security (WINS) ■ December 4, 2019
International Workshop on Countering Violent Extremism and the Insider Threat in the Nuclear Sector

Dr. Eric L. Lang, Director, PERSEREC

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

TO UNDERSTAND AND MITIGATE INSIDER THREAT: TECHNOLOGICAL FACTORS ARE IMPORTANT; **HUMAN FACTORS ARE MORE IMPORTANT**

"Where we're missing the boat, oftentimes, is on the human resource side...We have to find a way to identify, mark them ahead of time and say, 'hey listen, I know things are rough, you're having problems, but there's other options.'"[1]

1 William Evanina, Director, National Counterintelligence and Security Center (2017) Quotation from Meritalk.com, https://www.meritalk.com/articles/insider-threat-programs-miss-human-side-problem-bill-evanina-odni-cybersecurity

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/Corporate Espionage**
  e.g., insider provides classified info to an unauthorized group or steals intellectual property for personal gain
- **Extremism/Terrorism/Violence**
  e.g., radicalized insider turns violent
- **Vandalism/Disruption**
  e.g., vengeful insider harms the organization's computer system
- **Reliability Problems and Gross Negligence**
  e.g., insider with alcohol/substance abuse, psychological problems, or gross incompetence fails to protect sensitive info/systems

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

INSIDER THREAT PROBLEM: EXAMPLES & MAGNITUDE

Insider threat generally occurs in three varieties of decreasing frequency[1]

- Careless or uninformed insiders who **unintentionally violate security requirements** and policies due to a lack of motivation and/or ineffective cybersecurity training (resulting in low "cyber-hygiene" awareness).

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

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

[1]ICIT, 2017

INSIDER THREAT PROBLEM: EXAMPLES & MAGNITUDE

- "Cyber crime damages [across all sources] will cost the world $6 Trillion annually by 2021, up from $3 trillion in 2015," and "is the greatest threat to every [organization] in the world." (2017 State of Cybercrime)
- Problematic cyber-incidents are more often caused by insiders—by malice or negligence—than by external attackers.
- Among **malicious intentional** insider attacks:
  - 62% involved employees trying to benefit from their employer's sensitive data (while still on the job)
  - 29% stole information as they exited employment for future financial gain
  - 9% were saboteurs

INSIDER THREAT AT NUCLEAR FACILITIES AND LABS: EXAMPLES & MAGNITUDE

- 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 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-Qaeda 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 than $100 million in repairs)
- Difficult challenge of balancing openness and innovation benefits of hosting foreign students/faculty at research labs, with risk of academic espionage and exfiltration

KEY FINDINGS FROM PERSEREC RESEARCH ON DOD RESOURCE EXFILTRATION

"***The Resource Exfiltration Project: Findings from DoD Cases, 1985-2017***"
Broader case eligibility (compared to PERSEREC espionage trends reports):

- focus on incidents rather than prosecutions,
- include spies, leakers, hoarders,
- cover classified and unclassified (sensitive) government resources

- 2018 report confirmed others' findings from published literature:
  No consistent or useful **demographic** profile of a spy or exfiltrator
- Money/greed is still a lead motivator but has been decreasing over decades
- Increase in volunteering vs being recruited by a foreign entity
- Divided loyalties increasing over time; second only to money/greed

HOW THEY EXFILTRATED

Of 37 cases for which open source intelligence was available:

- **<u>27 of 37 (73%) did NOT rely on technology[1]</u>**
  - 17 perpetrators concealed resources in a container of some kind, usually a briefcase or bag
  - 7 perpetrators concealed resources on themselves (e.g., pocket, under hat)
  - 4 perpetrators misused courier card privileges
  - 11 perpetrators never physically exfiltrated anything; they worked from memory
- 10 perpetrators exfiltrated resources via email or fax

[1]*Total exceeds 27 because some perpetrators used multiple methods*

HOW DOES SOMEONE BECOME A RISKY INSIDER?

- **BASIC PSYCHOLOGY: Thoughts, feelings & behaviors come from:** Dispositional factors (e.g., personality & mental health) that interact over time with:
  - Individual events and stressors
  - Social, contextual and organizational influences
- **RADICALIZATION: The interplay of Needs, Narratives, Networks**
  - Meaning, dignity, belonging (often related to a “significance quest”)
  - A person’s evolving self-story of development, identity and life trajectory
  - Family, friends, work associates, religious group, social/community groups

BEHAVIORAL INDICATORS OF POTENTIAL RISK

1. Unwillingness to comply with rules and regulations or security requirements
2. Signs of alcohol abuse, drug misuse or illegal drug use
3. Apparent or suspected mental health issues
4. Criminal conduct or affiliation with criminals, violent groups or online radicals
5. Misuse of organizational property or systems, or inappropriate “work-arounds”
6. Unexplained affluence
7. Any behavior that raises doubts of reliability to protect National Security
8. Threatening language
9. Serious disloyalty or disinterest in the mission/needs of the organization or nation
10. Attempts to access files or facilities not clearly within their work responsibilities
11. A pattern of counterproductive work behaviors
12. A pattern of serious lying, evasiveness and defensiveness
13. 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)
14. **An inability or unwillingness to correct one’s own bad behavior**

***1-7 are reporting requirements per ODNI 2017 policy**

INSIDER THREAT SCIENCE-BASED INSIGHTS & BEST PRACTICES

1. 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

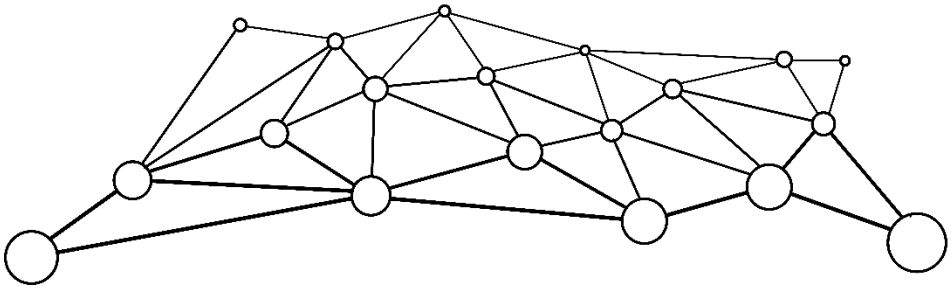
2. Initial personnel screening is critical but not sufficient. Continuous Evaluation "CE" (tailored for risk management) is more important. Insider Threat is more often a process than a single event.

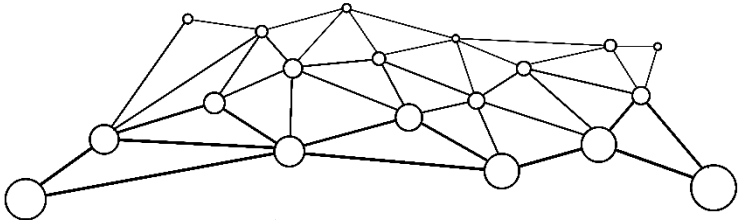
3. Organizations need to better develop, and communicate with employees, an effective, trust-based, atmosphere of the need for Insider Threat programs, individual's roles and how programs will be conducted fairly. Listen to and discuss employee concerns and questions. (e.g., 2018: 70% employees would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

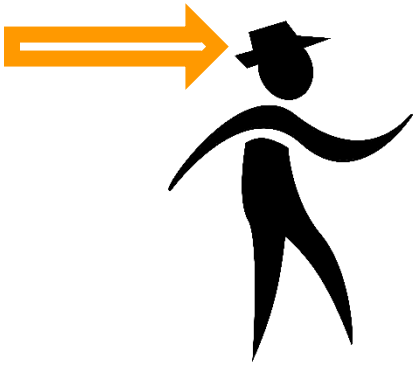
4. Organizations need to better understand office climates and cultures (e.g., levels of frustration, unfairness, toxic leadership, tolerance for rule-breaking, trust) and how these contexts exacerbate or mitigate Insider Risks. Most bad and good behaviors result from interactions of individual's dispositions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

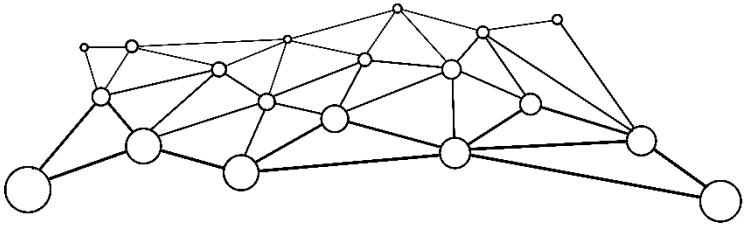
5. Need to integrate info from many relevant and privacy-appropriate sources, e.g., criminal, financial, travel, network user activity monitoring, supervisor/coworker reporting, social media; assessed by an Insider Threat team (i.e., an integrated NET for "Neutralizing Enterprise Threat"). Most important, Security and Human Resource personnel must work together.

WHY THE “NET” METAPHOR?









INSIDER THREAT SCIENCE-BASED INSIGHTS & BEST PRACTICES

6. 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.

7. 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/training, 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?”

8. Improve supervisor/coworker reporting. This is the biggest underutilized source of helpful info to mitigate Insider Threats, especially for indicators not assessed by UAM and database alerts. 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 (from an individual or organization)
  - Diffusion of responsibility

- 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, for example:
  - 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/
- PERSEREC research and tool for assessing risky personality disorders using "Dispositional Indicators of Risk Exposure" DIRE
- M. Bunn and S. Sagan's 2017 book "Insider Threats," which includes helpful analyses of relevant insider threat case studies
- A. Kruglanski & J. Bélanger 2019 book "The Three Pillars of Radicalization: Needs, Narratives, and Networks"

CONCLUDING THOUGHTS…

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., 2018 book “Weapons of Math Destruction” and “Frankenalgorithms” and 04Apr2019_”AI researchers slam Amazon for selling 'biased' facial recognition tech to cops”).

- 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

PERSEREC IS A U.S. DEPARTMENT OF DEFENSE (DOD) RESEARCH CENTER DEDICATED, SINCE 1986, TO CONDUCTING AND APPLYING…

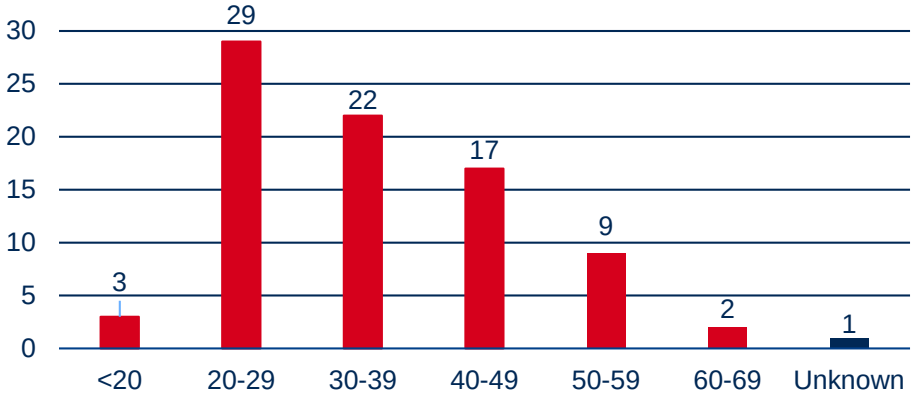
SOCIAL SCIENCE TO IMPROVE THE EFFECTIVENESS, EFFICIENCY, AND FAIRNESS OF PERSONNEL SECURITY, INSIDER THREAT, SUITABILITY, AND RELIABILITY SYSTEMS.

PERSEREC Insider Threat Research Areas relevant to improving policies & tools

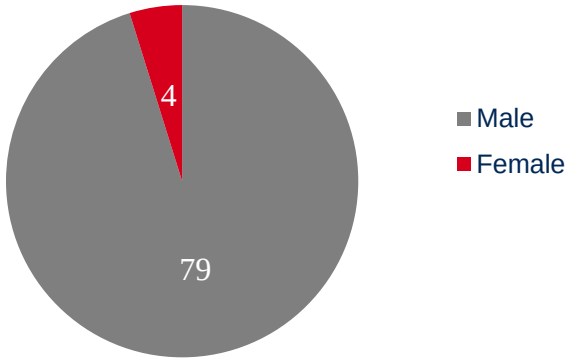
- Emerging threats, such as social media applications, for personnel risk
- Contextual and organizational factors that interact with individual dispositional factors to exacerbate or mitigate risk
- Automated tailored Continuous Evaluation "CE" of personnel
- Definitions and metrics for security vetting 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

DEMOGRAPHICS OF EXFILTRATORS

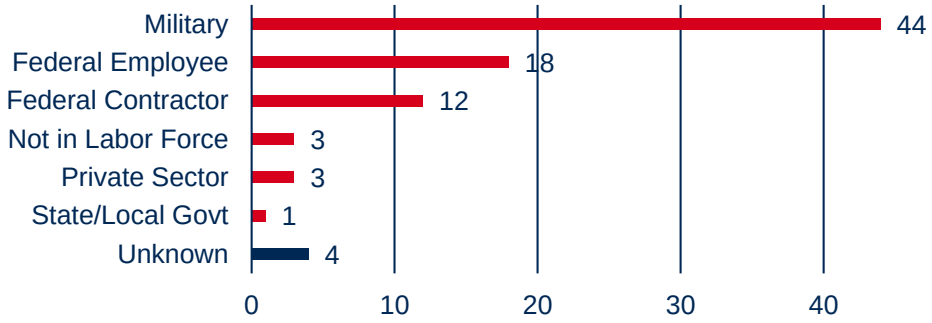
Age When Exfiltration Began (N=83)



Sex When Exfiltration Began (N=83)

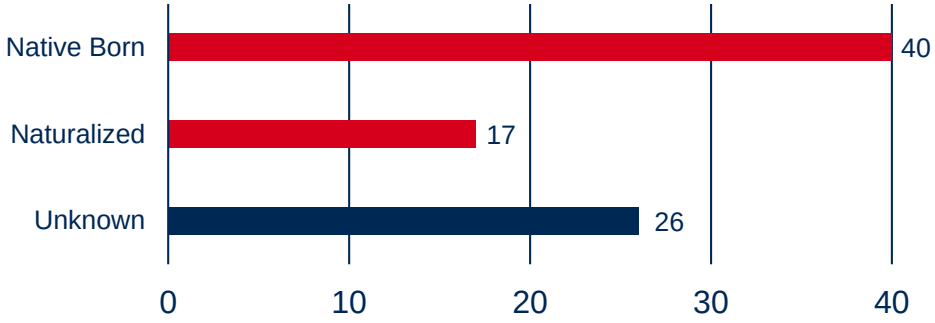


Occupation When Exfiltration Began (N=83)

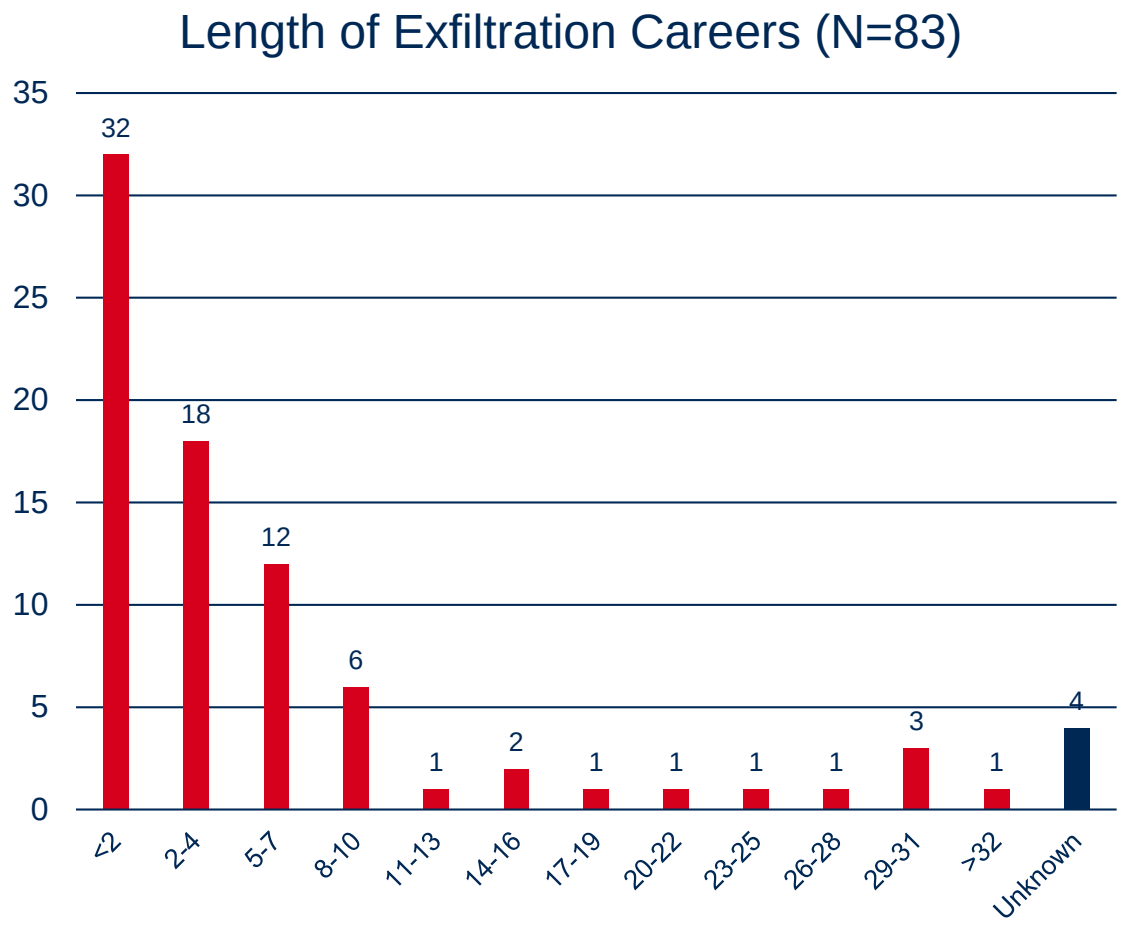


Total exceeds 83 because two perpetrators had multiple occupations when exfiltration began

Citizenship When Exfiltration Began (N=83)



MANY EXFILTRATED FOR SEVERAL YEARS



Of the 79 perpetrators for whom relevant open source intelligence was available:

- 32 perpetrators (41%) were active for less than 2 years
- 18 (23%) were active for 5-10 years
- Several (9%) were active for more than 20 years
- Of the four women included in this study, two had exfiltration careers that lasted longer than 10 years