Global Material Security

The Insider Threat

Justin R. Kinney, Ph.D.
R&D Associate, Oak Ridge National Laboratory
National Nuclear Security Administration
U.S. Department of Energy

National Nuclear Security Administration

U.S. DEPARTMENT OF ENERGY

Definitions

Global Material Security

- Insider: an individual "with authorized access to nuclear [or other radioactive] material, associated facilities or associated activities, or to sensitive information or sensitive information asset"
  (IAEA NSS No. 8-G (Rev. 1))
- An insider threat may use their **access, knowledge**, or **authority** to exploit/defeat/bypass security systems & attempt unauthorized removal or sabotage. This would turn them from a potential threat into an adversary.
- Important point: **legitimate, authorized** access to controlled areas
  - This list can include employees, former employees, contractors & consultants, venders, regulators & inspectors, first responders, or even visitors to a site

Definitions continued…

Global Material Security

Access: Authorized and capable of bypassing security measures in restricted areas. Includes physical access, computer access (even potentially remote access). Provides opportunity

Authority: Power/right to conduct operations, direct employees, enforce obedience, or utilize equipment/tasks

Knowledge: Potential targets for theft/sabotage, facility layout, how to acquire or use tools & equipment, security systems/measures

(Don’t necessarily need all three to perform a malicious act)

Extremism

Global Material Security

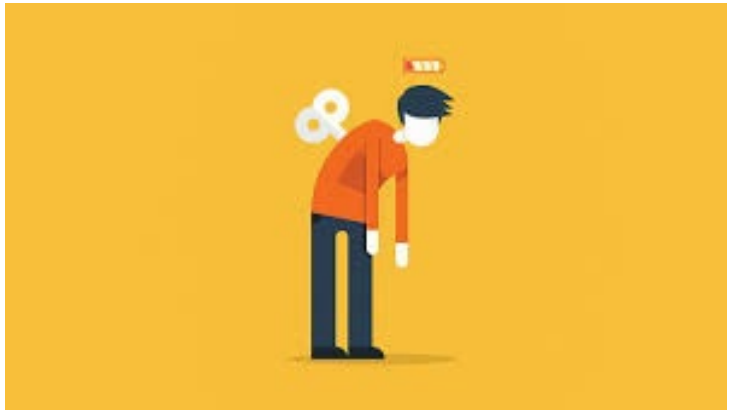
- Many psych motivations/paths
  - Fear, loneliness, perceived lack of opportunities, feeling like a victim

- Radicalization processes:
  - Emotional reasoning (Anger or fear amplification)
  - Target identification (directing hate)
  - Polarization (Us vs. Them mentality)
  - Separation/Isolation from ‘non-believers’ (often friends/family)
  - Social Support Group
  - Righteousness – Moral, ‘rights’

Kinds of Insider Threat: Unwitting

Global Material Security

- (aka, Pawns/Goofs)
  - Unintentional/Accidental
  - Non-hostile—No ill will
  - Training deficiency
  - Ignorance, Lack of attention, Distraction, or Negligence
  - Possibly due to illness or fatigue
  - Recklessness
  - Could be as simple as clicking a malicious link in an email or failing to check an alert because there have been false alarms lately
  - Often used as an instrument/pawn of an adversary



Kinds of Insider Threat: Malicious

Global Material Security

- (aka, Turncoats)
  - Intentional, Deliberate, Witting
  - Seeking to cause harm, Hostile
  - Theft of materials, information, or intellectual property
  - Sabotage of materials or systems
  - Could be a lone wolf
  - Could be a collaborator (in collusion with outsider threat/organization)
    - Recruited by adversary seeking to exploit an insider's access/authority/ knowledge
    - Or coerced into it.

Insider Motivations/Triggers to Act Maliciously

Global Material Security

- Ideological– radical, extremist conviction; religious or secular; ethnic or nationality; environmental. Divided loyalty.
- Financial– monetarily motivated, could be in a time of hardship due to medical bills or other financial commitments
- Ego– arrogance, testing their own abilities, narcissistic
- Psychotic– mental illness; functioning & capable, but there is an underlying instability
- Revenge– disgruntled employee (former employee) or customer, seeking to get back at the organization for a perceived slight (passed over for promotion/negative evaluation)
- Coercion– threats from an adversary, either to themselves, their family, or others they care about. Could be physical harm, reputation, or otherwise.

Passive vs. Active Insider Threats

Global Material Security

- Passive
  - Not willing to commit an act of violence or hurt people
  - Usually provide basic information in order to help **outside** adversaries gain access or perform a malicious act
  - E.g. failing to lock a door, leaving a computer logged in & unattended, giving out a password

- Active
  - Usually non-violent as well, but *can* become violent, depending on the circumstances
  - Provide information, but also willing to perform actions
    - Open doors, tampering, engage response personnel
    - The more active in the threat, the less likely to care about getting caught/losing their job/etc.

Case Study: Glenn Michael Souther

- Navy photographer, later Reservist at a secure facility processing satellite recon photos
- Defected to the USSR in 1986
  - Passed information/photos on weapons, movements, nuclear strike criteria
- Motivations: Disillusioned w/ his job, ideology, money
- Recruitment: Volunteered to work for Soviet intelligence services
- Accessing Information: Through his normal duties & took advantage of lax security
- Colleagues failed to report multiple indicators: unusual work hours, undue affluence, suspicious foreign travel, etc.
- Background check failure
  - Discounted reports from ex-wife about his instability and defection.

Radiological/Nuclear Insider Threat Case Studies

Global Material Security

Who	When	Where	How	Why	Mitigation Recommendation
Hacker who sent email to researchers, posing as a student	November 2015-June 2016	University of Toyama's Hydrogen Isotope Research Center, Japan	Malicious email attachment was accidentally opened, giving access to personal info and data	Insiders – Unintentional Hacker -- Unknown	Cyber Security training Anti-phishing software/email settings
Two insiders: Former Administrative Director and a driver	April 2014	Sogetrap Facility in Algeria	Two-insider team stole a Gamma Densimeter with radioactive source	Unspecified	Off-boarding policies – revoking access to former employees --Physical security to make device less portable
Four employees & four outsiders	February 2017	Oil & Gas Exploration Company, Malaysia	Stole two gamma projectors with iridium-192 were stolen using a company van	Financial Gain	Rules on vehicle storage Improved physical security

Threat Assessment: Targets

Global Material Security

- Theft or Sabotage Targets
  - Radiological or Nuclear Material
  - Buildings or Equipment
  - Components or Systems
  - Transportation processes
- Information
  - About the facility, employees, personal information, or the work being performed there
- Intellectual Property
  - Patents, Plans, etc.

Thought Experiment

Global Material Security

How might an insider threat with malicious intent obtain knowledge regarding a RAD shipment & use that knowledge to carry out an attack?

Times of transport are among the most vulnerable for anything, but especially for high-value, high-risk items like radiological/nuclear material.

Knowing how, when, where this material is being moved could be very useful information for an insider threat

What are the Signs?: Behavioral Indicators

Global Material Security

- Vocal disagreements with policy
  - With corporate, managers, federal policy
- Absenteeism
- Angry/hostile arguments w/ coworkers
- Bullying/manipulative behavior
- Addictions
  - e.g. Alcohol, Drugs
- Financial distress
  - Personal or family issues
- Extreme interest in projects outside their scope

Recognition: What are early warning signs?

Global Material Security

- Virtual/Computer Indicators
  - Change in regular working hours
    - Online at unusual times
  - Accessing data they don't usually access
    - Times, locations, etc.
  - Downloading large amounts of data
    - Particularly if they have minimal reason to work with that data
  - Unauthorized storage access

    (e.g. USB sticks)

Reaction: Preventive Measures

Global Material Security

Used to reduce number of insiders OR minimize opportunities

- Identity verification
  - Access Control & Multi-level Identity Scans
- Trustworthiness assessment
  - Background checks (Initial AND continued monitoring), Identity Verification
  - Clearance screenings, Trustworthiness assessments
    - Risk of 3rd party suppliers/providers who may not have the same checks
- Escort/surveillance
  - Cameras with active monitoring, multiple personnel
  - Two-person rule, to avoid employees accessing secure areas alone. Both preventive and protective
- Security awareness
  - Better/Increased training – physical and cyber security

More preventive measures

- Confidentiality
  - Different levels of access
- Quality assurance
  - Oversight
- Employee satisfaction
  - Positive Working Environments
  - Employees must feel valued, respected, & heard
- Compartmentalization (of data, activities, and physical areas)
- Separation of Duties
  - Keeps any single person from knowing too much
- Sanctions
  - For violations

Monitoring Levels

Global Material Security

- Company Monitoring
  - Alarms, Regular inspections, anti-phishing software/settings
  - Tracking personnel
    - ID cards, checkpoints, etc.
  - Background Checks/Security Clearances
    - Behavior disorders, mental illness, criminal history, financial problems, family problems

- Employee Monitoring
  - Peer recognition of abnormal or harmful behavior
  - Coworkers are in the best position to notice aberrant behavior or the personal struggles of one another
    - So use them! Give them training to recognize signs and the ability/license to react or report, as appropriate for their role.
    - Sometimes all it takes is one person to notice when a coworker is struggling and to be a good friend

Protective Measures

Global Material Security

- GOAL: Detect/Delay/Mitigate/Reverse the threat
- Stop acquisition (theft) or sabotage of materials, or at least slow them down to allow response personnel to arrive
  - Locks, multiple levels of security, barriers that require special tools/skills or extra personnel, etc.
  - Delay until security personnel can respond
- All employees should be trained to react and send information alerts, as necessary for their roles
  - Empower everyone in the organization to help secure the premises/materials
  - De-escalation measures

De-Escalation Measures

- Engaging People/Talking to them
  - This lets someone know you're aware of their presence
    - Also builds a good organizational culture of support that strengthens cohesion
  - Communication

- All employees can be taught & trained in de-escalation techniques.

- Building established, trusted relationships is key for threat management. Friends, family, and close coworkers are critical to noticing concerns.

Layered Defense Measures

Global Material Security

- Technical Measures
  - Sensors & Alarms
  - Closed Circuit Monitoring (CCTV)
  - Locks/Barriers at multiple levels
  - Reporting systems

- Administrative Measures
  - Screening/Training
  - Awareness of surroundings (Empower all employees in this capacity)
  - Observation/Reporting
    - Provide safe, reasonable avenues for employees to anonymously report anything they see that is suspicious

Stages of Prevention & Protection

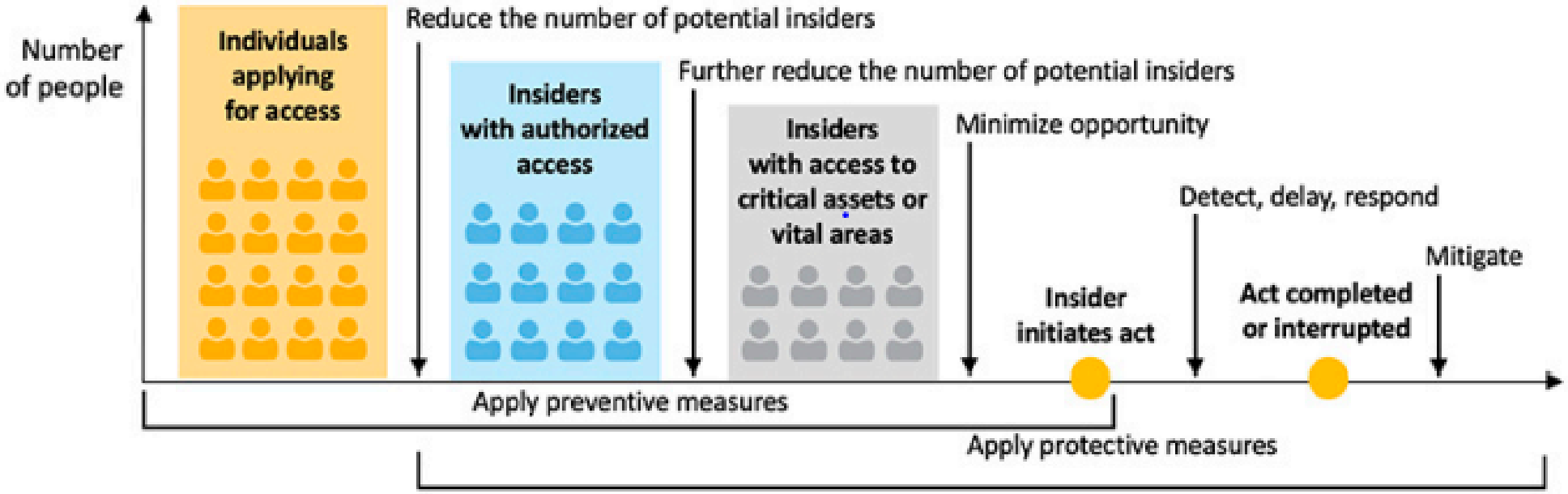


FIG. 1. Steps for using preventive and protective measures against potential insider threats.

IAEA Nuclear Security Series No. 8-G (Rev. 1): Preventive and Protective Measures against Insider Threats

Secondary Threat: Transnational Criminal Organizations (TCOs)

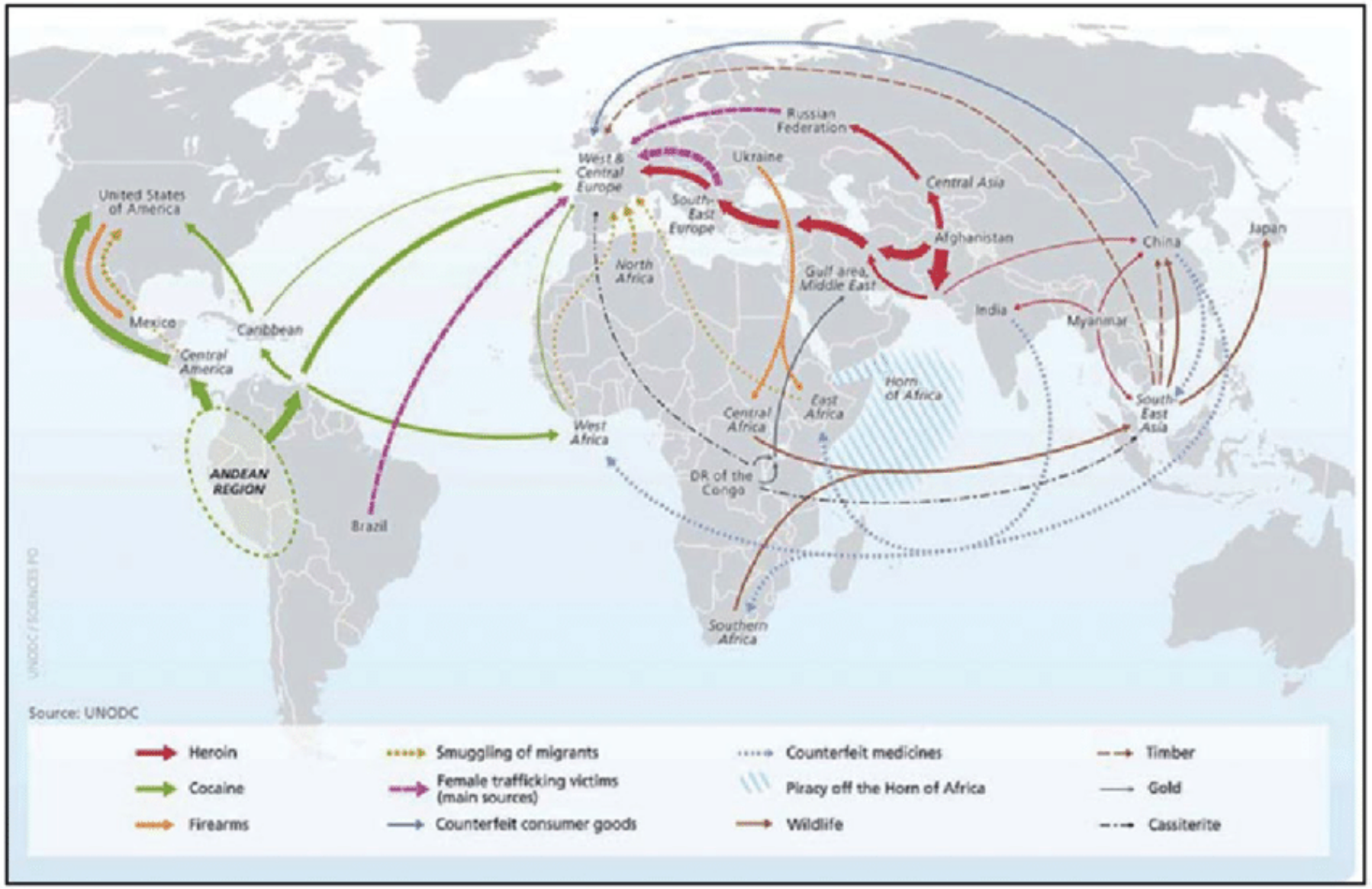
Global Material Security

- International criminal groups that traffic drugs, humans, and/or other items illegally
- Established pipelines to buy/sell products
- Because they have established routes that they know work, other criminal organizations like to use them to traffic their own goods
  - Drugs, humans, black market, etc.

- THOUGHT EXPERIMENT: What if TCOs and extremist groups work in collaboration?
  - How could an insider be used in a case like that?
  - Theft of items using insider status, sold via TCO chain on the black market

Established TCO Smuggling Routes

Global Material Security



Solutions/Summary

Global Material Security

- IMPORTANT: Not a one-size-fits-all solution to insider threats
- Unfortunately, there is no simple, all-encompassing motivation, nor a universal indicator of the potential problem, nor a single response that works in all cases.
- Each instance is unique to the specific facility, atmosphere, and the employees who work there
- However, there are prevention, protection, mitigation, and response techniques that can be employed to minimize risk at different stages
  - Technical vs. Administrative
  - Deterrence vs. Detection vs. Response

Questions/Comments