2022 WEBINAR SERIES

# Risk Management's Role in Mitigating the "Insider Threat" Security Risk

UTHealth Houston

Robert Emery, DrPH, CHP, CIH, CBSP, CSP, CHMM, CPP, ARM
Vice President for Safety, Health, Environment & Risk Management
The University of Texas Health Science Center at Houston
Professor of Occupational Health
The University of Texas School of Public Health
Robert.J.Emery@uth.tmc.edu

UTHealth

# Learning Objectives

- Define “insider threats” and how they differ from threats external to an organization
- Identify the different types of insider threats
- Provide examples of damage that can be caused by insiders - specifically addressing health & safety threats
- Identify the steps risk management professionals can take to help mitigate the risks associated with insider threats
- Provide a list of useful references

# How Many Times Have We Heard This after an event?

*You know, s/he had been acting a little strange, but….*

*…I didn't think much of it…*

*…I never bothered to report it…*

*…I didn't know who to report it to…*

# Why a Presentation on Security to Risk management Professionals?

- Post 9/11/01, the safety and security professions have forever become intertwined
- Both are focused on controlling losses – the key difference is “intent”
  - Only in the English language are there different words for “safety” and “security” – everywhere else it means the same thing
- Emergence of many regulations that include now security elements
  - Increased controls for radioactive materials in quantities of concern
  - Select agents and toxins
  - CFATS
  - Transportation security requirements for hazardous materials/wastes
- In the course of risk management’s daily activities (if trained appropriately), opportunities exist to enhance security within an organization, especially with regard to insider threats

# External vs. Internal Threats

- Organizations commonly maintain a variety of systems to prevent threats external to the organization from gaining access to steal or damage property or reputation
  - Historically known as the “3 G’s”: Gates, Guards, and Guns
  - External attempts to physically or electronically access organizations are regularly detected and thwarted

- The risk that is much harder to detect and control is the “insider” – the employee or contractor who has gained legitimate access, but now, either intentionally or unintentionally, represents a risk

# First: a Word About Insider Threats and Workplace Violence

- Not limited to workplace homicides so widely covered in the news
- Defined as:
  - *an act against an employee that creates a hostile work environment and which negatively affects the employee, either physically or psychologically. These acts include all types of physical and verbal assaults, threats, coercion, intimidation, and all forms of harassment*

- Workplace Violence Research Institute

# Workplace Violence

- How extensive is the threat?
  - 1 of 4 employees harassed, threatened, or attacked on the job
    - Northwestern Life Insurance Co.
  - 50% of companies surveyed reported experiencing workplace violence in last 4 years
    - American Management Association
  - Average of 1,100 workplace homicides annually
    - U.S. Department of Justice

# Workplace Violence Prevention Program Elements

- Form a management team
- Assess current conditions – controls, culture, etc.
- Prepare and implement policies
- Establish confidential means for collecting information (a hot line)
- Develop a training program for all employees
- Provide supervisor and managers with conflict resolution training
- Review pre-employment screening practices
- Review termination process
- Prepare a crisis response plan
- Test and update program regularly

# Different Types of Insider Threats

- Malicious insider
  - Nefarious intent
- Coerced or sympathetic insider
  - Actions caused by external forces
- Oblivious insider
  - Unaware of the impact of their actions or inactions

# What is at Risk?

- Money/assets (insiders cost businesses >$100 Billon annually!)[a]
- Personal information
- Trade secrets
- Critical records, data
- Business information
- Organizational reputation
- Customer base
- Health & safety of workers and/or public

[a]Winkler, I. Spies Among Us, p. 60

# Specific Health & Safety Risks

- Access to potentially hazardous chemical, biological, or radiological materials for either malicious purposes (themselves, co-workers or the public), or to damage the organization's reputation resulting in regulatory scrutiny and penalties
- The purposeful disruption of critical safety systems
- Purposeful deletion of critical records
- Release of selected information to damage reputation or to further a cause

# Typical Controls

(and who controls them)

- Background and reference checks as part of hiring process
- Employee training and orientation
- Organization policies and procedures
- Access controls – both physical and virtual
- Auditing, security reviews
- Corrective action plans, termination processes

# Are These Controls Sufficient?

- The answer: Not always. Consider a few examples:
  - Animal rights groups placing undercover employees in research labs and factory farms to document the treatment of animals and in some cases release the animals and damage property.
  - Software engineer, about to be laid off, copies for his own purposes, and then deletes, source code for a safety-related system being used in production. After detection, arrested and convicted: 1 year in prison, $13,000 fine

# Radiological Examples 1995 -1998

- Report to Congress on Abnormal Occurrences which occurred between July and September 1995, 3rd Event: NIH Incident, Federal Register, February 26, 1996, Vol. 61, No. 38, pp.7123-7124.

- US Nuclear Regulatory Commission, NUREG 1535, Ingestion of Phosphorous-32 at MIT, Cambridge MA, Identified on August 19, 1995

- US Nuclear Regulatory Commission, Preliminary Notification of Event or unusual Occurrence PNO-1-98-052. Subject: Intentional Ingestion of Iodine-125 Tainted Food (Brown University), November 16, 1998.

- March 1998, routine inventory of radioactive sources revealed that 19 Cs-137 sources missing from a reportedly secured room in a Greensboro, NC hospital. Sources are never recovered

# How Serious is the Threat of Insiders?

- The Federal Reserve Bank of New York requires individuals in sensitive positions to be absent from work for two consecutive weeks each year, with no electronic access!
    - *"One of the many basic tenets of internal control is that a banking organization ensure that employees in sensitive positions be absent from their duties for a minimum of two consecutive weeks. Such a requirement enhances the viability of a sound internal control environment because most frauds or embezzlements require the continual presence of the wrongdoer."*
- Also suggests regular rotation of jobs and duties

http://www.newyorkfed.org/banking/circulars/10923.html

# What might Drive One to Become an Insider Threat?

- According to the FBI, there can be:
  - Personal Factors
  - Organizational Factors

# Personal factors

- Greed or financial need
- Anger/revenge
- Problems at work, disagreements
- Ideology/identification
- Divided loyalty
- Adventure/thrill
- Vulnerability to blackmail
- Ego/self image
- Ingratiation – desire to please
- Compulsive or destructive behavior
- Family, personal problems

# Organizational Factors

- Availability and ease of accessing critical information, equipment, supplies
- Proprietary or classified information not labeled or handled as such
- Undefined policies regarding work from home on sensitive or propriety projects
- Time pressures
- Employees not trained on how to protect proprietary information and on security risks

# Behavioral Indicators of Insider Threats

- Taking items home without need or authorization
- Seeks information, supplies not related to job
- Expresses interest in matters outside scope of job
- Unnecessarily copies materials
- Disregards company policies on computer use
- Works odd hours
- Unreported foreign contacts, short trips to foreign countries
- Unexplained affluence
- Overwhelmed by life crises or disappointments
- Unusual interest in personal lives of others
- Concerns about being investigated, under surveillance

# What Can Cause a Good Person to Turn Bad? Things You Might Never Know

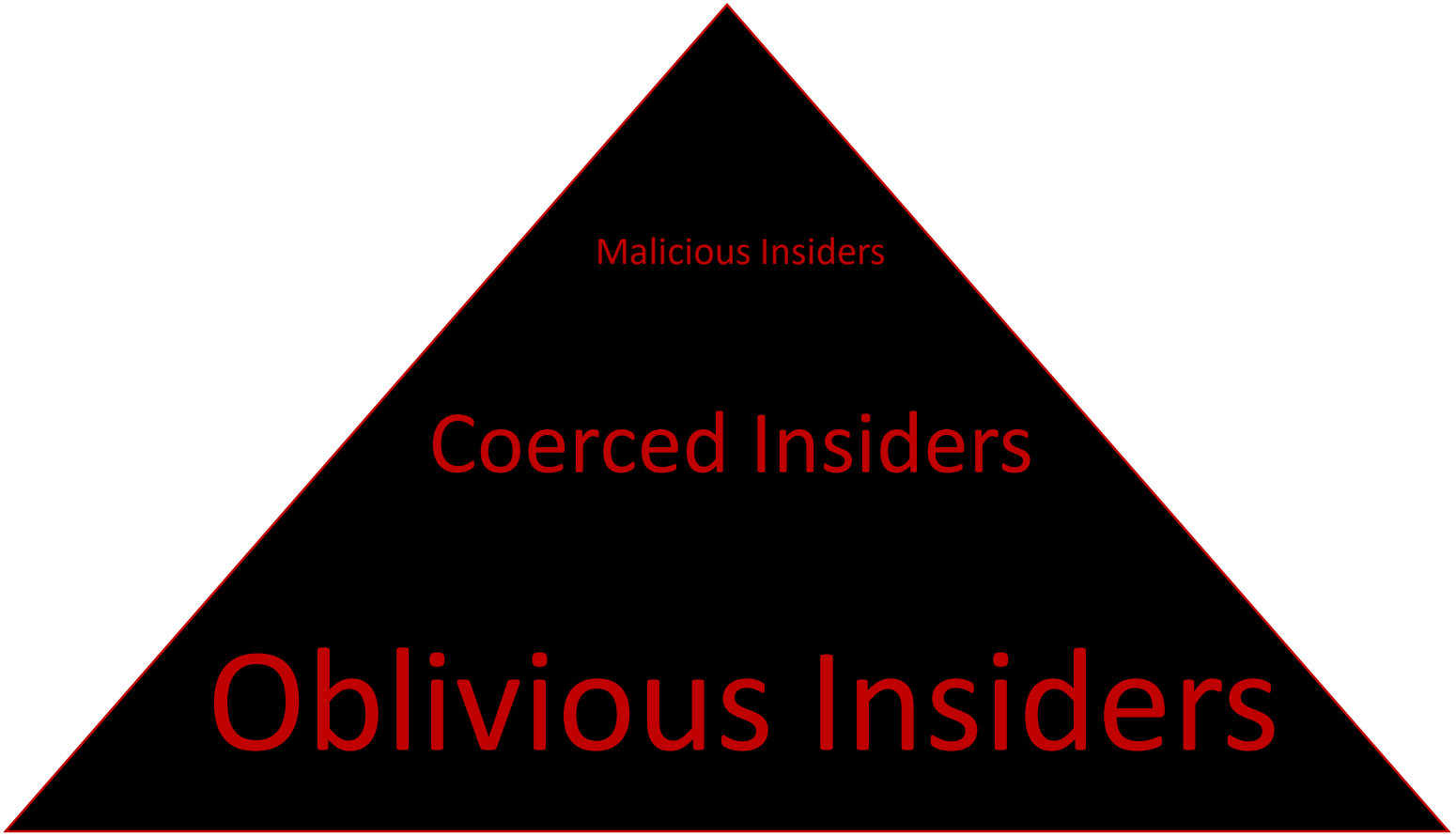
- Individuals can become a coerced insider because of:
  - Financial pressures – debt, gambling, loans
  - Inappropriate or deteriorating relationships
  - Embarrassment
  - Scams, get rich quick schemes
  - Extortion, even from afar if pressures are being applied in home country
  - Personal problems, substance abuse, stress
  - Changes in personal beliefs, disillusionment
  - Siloed information sources: “the echo effect”

# Here's The Challenge….

- From actual National Security Agency documents –
  - *"Exhibits an interest in what co-workers are doing"*
  - *"Volunteers for extra duties and assignments"*
  - *"Works late hours"*
  - *"Rarely takes vacations"*
- Characteristics of a good employee or an insider?

Winkler, I. Spies Among Us, p. 61

# Insider Threats by Relative Populations



# Oblivious Insider

- Examples
  - Writes down or posts passcodes for convenience
  - Props doors open, bypassing locks, to save time
  - Holds doors open for others, letting tailgaters in
  - Vulnerable to “social engineering”

- May be a much greater threat than the Malicious Insider because of
  - Sheer numbers
  - Repeated acts
  - Misconception of actions
  - Difficulty of detection and mitigation


Source: GAO.

Figure 3: Combination to Lock on Door Frame Outside Blood Bank

Source: GAO.

- At a blood center in a third state we visited, we observed a cesium-137 blood irradiator of approximately 1,400 curies in a room that was secured by a conventional key lock. The irradiator was located in the

Page 17 GAO-12-925 Nuclear Nonproliferation

GAO-12-025 Nuclear Nonproliferation Report

# Risk Management's Unique Position

- Some significant proportion of risk management's work is done in the field, with regular interactions actually in the workplace
- It is routine for risk management to maintain a dialogue with the workers, reporting of concerns
- Risk management generally understands entire systems as part of their assessment work
- Risk management's involvement with maintenance of inventories of materials on site
- There is often an elevated level of worker trust with risk management personnel when the issue of "dual loyalty" is handled appropriately

# What Can Risk Management do?

- Educate risk management staff about the insider threat risk, the factors that can lead to its existence, and the suspect behaviors, and where to report them

- Increase situational awareness, especially during routine safety surveillance
  - Locks bypassed, tailgating, passcodes posted?
  - Unusual behaviors? Know your customers!

# What can Risk Management Do?

- Actively solicit worker safety and security concerns
- Review of access data logs
  - failed attempts, odd times?
- Perform inventories from the perspective of shrinkage
- Get on the notification roster for terminations
  - take necessary protective steps (change passcodes, delete badges, inform parties so they can report if the person is attempting to return)
- Report suspicious activities or situations
  - "see something, say something" – but the key here is see what? Tell whom?

# Important point!

- *"Insider threat mitigation is focused on behavior – not assumption!"*

T. Engells, Chief of Police UTMB

# Once a Report is Received, What Happens Next?

- A Behavioral Intervention Team (BIT) may be engaged, which is a multi-disciplinary group whose purpose is meeting regularly to support its target audience via an established protocol.
- The team tracks “red flags” over time, detecting patterns, trends, and disturbances in individual or group behavior.
- If a BIT receives reports of disruptive, problematic or concerning behavior or misconduct (from co-workers, community members, friends, colleagues, etc), conducts an investigation, performs a threat assessment, and determines the best mechanisms for support, intervention, warning/notification and response. The team then deploys its resources and resources of the community and coordinates follow-up.
- BITs intervene with specialized knowledge to identify the earliest signs of potential crisis rather than waiting for clear signs of an impending threat and reacting.
- BITs develop success plans for employees that may include disability support, treatment requirements, and other assistance.
- BITs focus on training front line employees, supervisors, and designated staff on behavioral recognition and identification of warning signs and red flag behaviors.

# A Note About Cyber Security

- Two ways to conduct research and development
  - Invest and perform R&D work, or just steal it
  - FBI estimates $13 Billion in annual losses due to economic espionage
- Wall Street Journal report: The State of Michigan's computer infrastructure experiences 185,000 cyber attacks daily

# Suggested Mitigation Elements for Insider Cyber Threats

1. Consider insiders in enterprise risk assessments
2. Document and consistently enforce policies and controls
3. Provide threat awareness training
4. Review hiring process, responding to disruptive behavior
5. Anticipate and manage negative issues in the workplace
6. Know your assets
7. Strict password policies
8. Enforce separation of duties
9. Define cloud service security
10. Stringent access controls
11. Institutionalize system change controls
12. Use log correlation engines to audit worker actions
13. Monitor and control remote access points
14. Develop a comprehensive employee termination procedure
15. Implement secure backup and recovery processes
16. Develop a formalized insider threat program
17. Establish a baseline for normal network behavior
18. Be vigilant about social media
19. Close the doors to exfiltration

# Summary

- Insider threats are very real and are difficult to detect
- Insiders may be after money or information, but their acts can also represent a risk management threat
- Keep in mind that although malicious insiders may exist, in general, they are far outnumbered by the oblivious insiders
- Through increased awareness, risk management can enhance security by helping identify possible insider threats to the organization

# References

- In addition to those listed in the presentation slides:


  - Colson, SC. Insider Threats 2.0: The Oblivious Insider, A Case Study. Syracuse University School of Information Studies 2009.
  - Emery RJ, Savely S. The benefits of actively soliciting worker concerns during routine safety inspections. Prof Saf 42: 36-38; 1997.
  - Silowash, G. et al. Common Sense Guide to Mitigating Insider Threats, 4th Edition. Carnegie Mellon University. Available at http://www.sei.cmu.edu/reports/12tr012.pdf
  - US Department of Justice Federal Bureau of Investigation. The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy. Available at http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure
  - Winkler, I. Spies Among Us: How to Stop Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day. Wiley Publishing 2005.

# 2022 WEBINAR SERIES

UTHealth Houston