## Identifying and Preventing Insider Threats

### Matthew D. Waters, Eastern Kentucky University

**Mentor:** Dr. Ryan Baggett, Homeland Security Program

### Insider Threats

- **Two Basic Types**
  - Adversarial
  - Unintentional

- **Insider Threat Working Definition**
  - Employee (past or present)
  - Permissible access
  - With or without malicious intent
  - Significant damage to the company and its reputation

### Identifiable Characteristics, Behaviors and Motivations

- **Characteristics**
  - No single profile
  - Predominately male
  - Prior arrests
  - Feelings of frustration
  - Permanent positions
  - Lack of empathy
  - Introversion
  - Reduced loyalty
  - Drinking/drugs/gambling
  - Low self-esteem
  - Impulsive
  - Manipulative

- **Observable Behaviors**
  - Computer dependency
  - Irregular IT activity
    - Complete violation of security protocol
    - Creation of backdoor pathways
    - Inappropriate social interactions
    - Language change
      - Aggressive hostile
      - First person personal pronouns

- **Motivation**
  - Revenge
  - Personal gain
  - Lack of loyalty
  - Response to negative life event
  - Negative interaction with employee
  - Laziness

### Preventative Means

- **Technology**
  - Intrusion Detection Systems (IDS)
  - Honeypot technologies
  - Auditing and authorizing

- **Non-Technological Means**
  - Risk assessments
  - Risk management framework
  - Threat assessment
  - Vulnerability assessment

- **Holistic Approach**
  - Policies
    - No “one size fits all” solution
    - Clear communication/properly posting policies
    - Punishment and deterrence
  - Training
    - One of the “greatest non-technical measures”
    - Recognizing characteristics, behaviors, and motivations
    - Understanding the programs and levels of security are necessary
  - Ad campaigns
    - DHS: “If You See Something, Say Something”
  - Legal issues
  - Human Resources
    - First line of defense against insider threats
    - Screening: background checks on employment, criminal, and financial histories
    - Establish a psychological baseline
      - All employees handling classified/sensitive information must meet this baseline

### Conclusions

- Insiders pose a growing threat
- Insiders can be identified by observing and analyzing characteristics, behaviors and motivations
- Technology plays a key role, but is not the sole answer
- Companies can and should utilize risk, threat, and vulnerability assessments
- Companies must take a holistic approach through policy implementation, proper training, ad campaigns, and an efficient human resources department

### References