

Identifying and Preventing Insider Threats

Matthew D. Waters, Eastern Kentucky University

Mentor: Dr. Ryan Baggett, Homeland Security Program



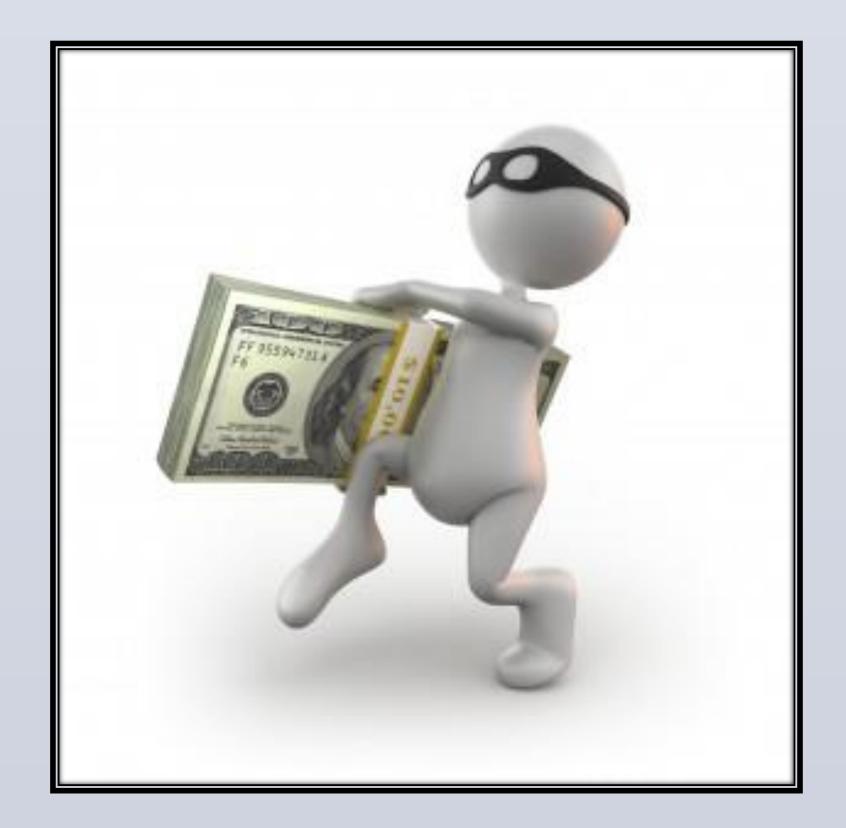
HOMELAND SECURITY

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

Topic Importance

- Greatest threat to information assets
- Frequency of attacks increases each year
- Monetary Damages
 - 50 times greater than external attacks
 - Approximately \$2.7 million per attack
- Most companies are unprepared
 - Lack of policies and procedures
 - Complex structures



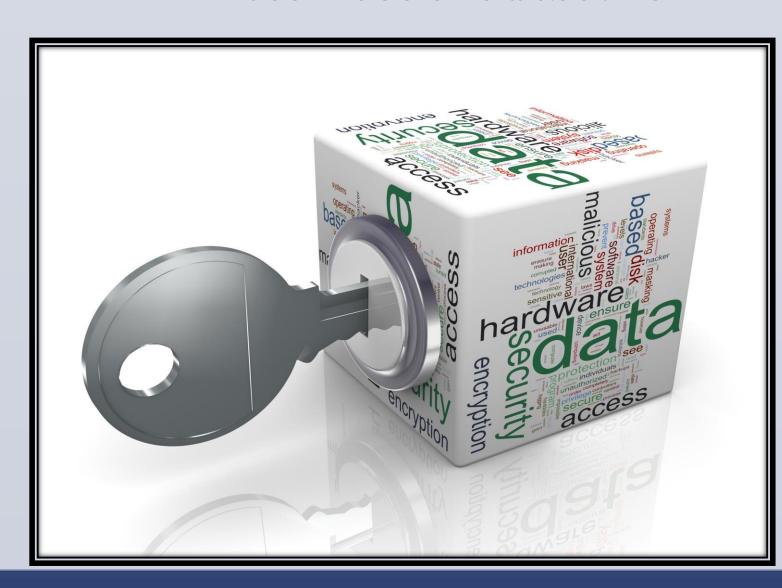
Identifiable Characteristics, Behaviors and Motivations

- 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

- Andrews, M., Thompson, H. H., & Whittaker, J. A. (2004). Intrusion detection: Perspectives on the insider threat. *Computer Fraud & Security*, 2004(1), 13. doi:10.1016/S1361-3723(04)00018-1
- Ball, L. J., Dando, C. J., Jenkins, M. C., Menacere, T., Ormerod, T. C., Sandham, A., & Taylor, P. J. (2013). Detecting Insider Threats Through Language Change. *Law & Human Behavior (American Psychological Association)*, *37*(4), 267-275. doi:10.1037/lhb0000032
- CERT Insider Threat Team. (2013). *Unintentional insider threats: a foundational study*. Retrieved from https://www-hsdl-org.libproxy.eku.edu/?abstract&did=741559
- Colwill, C. (2009). Human factors in information security: The insider threat Who can you trust these days?. *Information Security Technical Report*, *14*(4), 186-196. doi:10.1016/j.istr.2010.04.004
- Liang, L., Jeong, D. H., Yu, B., & Zeadally, S. (2012). Detecting Insider Threats: Solutions and Trends. *Information Security Journal: A Global Perspective*, 21(4), 183-192. doi:10.1080/19393555.2011.654318
- Spitzner, L. (2003). *Honeypots: catching the insider threat*. Retrieved from
- http://craigchamberlain.com/library/insider/Honeypots%20-%20%20Catching%20the%20Insider%20Threat.pdf
- Steele, S., & Wargo, C. (2007). An Introduction to Insider Threat Management. *Information Systems Security*, *16*(1), 23-33. doi:10.1080/10658980601051334
- United States Department of Homeland Security. (2010). *DHS* risk lexicon. Washington, DC: Government Printing Office.