References:

1. https://www.darkreading.com/vulnerabilities---threats/8-surprising-statistics-about-insider-threats/d/d-id/1326653?
   Article by: Ericka Chickowski
2. https://www.isdecisions.com/insider-threat/statistics.htm
3. https://www.isdecisions.com/compliance/manage-access-personal-data-GDPR-compliance.htm
4. https://www.isdecisions.com/role-file-auditing-compliance/
5. https://www.observeit.com/insider-threat/
6. https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat.pdf

Other Online Resources:

2017 Insider Threat Intelligence Report by Dtex.
https://www.thehaguesecuritydelta.com/media/com_hsd/report/154/document/2017-Insider-Threat-Intelligence-Report.pdf

Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey
https://www.sans.org/reading-room/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890

In 2017, The Insider Threat Epidemic Begins
http://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In-2017-The-Insider-Threat-Epidemic-Begins.pdf

Security Investigation Detection and Rapid Response with Splunk Enterprise
https://www.splunk.com/en_us/form/security-investigation-detection-and-rapid-response-with-splunk-enterprise.html?ac=ga_usa_comp_publicsector_threathunting&_kk=insider%20threat&_bk=insider%20threat&_bt=251113819820&_bm=p&_bn=g&gclid=Cj0KCQiA5aTUBRC2ARIsAPoPJk8oiWvPP8EjFVgWMbYF1A0hrCdkiwp4IEBmNc9XvWJgQX1Py2xyAIQaAm65EALw_wcB

Common Workplace Investigation Mistakes
http://www.informationweek.com/whitepaper/security-monitoring/security-management-and-analytics/common-workplace-investigation-mistakes/394983?cid=dlrr9&_mc=dlrr9

Danger Within: Unmasking Insider Threats
https://www.cyberark.com/lp/insider-threats/?utm_source=google&utm_medium=paid_search&utm_term=insider%20threat&utm_campaign=na_insider_threat_en&gclid=Cj0KCQiA5aTUBRC2ARIsAPoPJk-QJ8e-Ns5ICIh9m7UY7XM9B3LSNZ74ccjj8SFKDrM8u8rLkZmvoT8aAqBfEALw_wcB

Behavior that could indicate Insider Threat:

Identifying behavioral indicators may be difficult, particularly if they do not occur for a long period of time and therefore do not set a pattern. Therefore, a good understanding of risk characteristics and events that may trigger those characteristics is essential. Individuals pose threats for a variety of reasons; some theories to consider are listed below:

Make Chart:
Heading: Some Behavior Prediction Theories To Consider

Column 1	Column 2
General Deterrence Theory	Person commits crime if expected benefit outweighs Cost of action
Social Bond Theory	Person commits crime if social bonds of attachment, commitment, involvement and belief are weak
Theory of Planned Behavior	Person's intention (attitude, subjective norms and perceived behavior control) towards crime key factor in predictive behavior
Situational Crime Prevention	Crime occurs when both motive and opportunity exist

These behaviors may manifest in different stages of an insider threat scenario. Some commonly accepted stages include: Exploration (Recruitment/Tipping Point); Experimentation (Search/Reconnaissance); Exploitation (Utilizing the Weakness); Execution (Collection/Exfiltration); and Escape & Evasion (Obfuscation). Understanding these stages may help organizations put individual risk characteristics and behavioral indications into the context of an insider threat as the activity is occurring rather than after.

These behaviors and indicators, whether detected via technology or human observance techniques are intended to detect the malicious insider. It's equally important though to create productive and healthy work environments to help reduce the unintentional insider threat. Some countermeasures include:

- Train employees to recognize phishing and other social media threat vectors
- Train continuously to maintain the proper levels of knowledge skills and abilities
- Conduct training on and improve awareness of risk perception and cognitive biases that affect decision making
- Improve usability of security tools
- Improve usability of software to reduce the likelihood of system-induced human error
- Enhance awareness of the unintentional insider threat
- Provide effective security practices (e.g. two factor authentication for access)
- Maintain staff values and attitudes that align with organizational mission and ethics (6)

Finally, continual training is always a recommended option. Below are descriptions of two, free of charge courses that organizations may want to consider offering employees, contractors, and others that meet the description of an 'insider'.

- The Department of Homeland Security (DHS) offers an online independent study course titled guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats.
- The Department of Defense (DoD) also offers an Insider The course includes a printable certificate after completion and focuses on the insider threat as an essential component of a comprehensive security program.

Just as it is vital to have methods to detect external threats, it's also important to protect your organizations information and systems from unauthorized insider misuse. US-CERT recommends that organizations use the information and references in this product as tools to improve procedures employed to combat insider threats. (6)

Access, Security, and Audits – Oh My!

Presented by: Ute Kragl
DoD Compliance Officer
(kragl.u@gmail.com)

Insider Threat Reference Material & Handout
(Slides available upon request)

Threats can come from any level and from anyone with access to proprietary data!