Combating the Insider Threat

2 May 2014

Executive Summary

An insider threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.[1] Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware they are aiding a threat actor (i.e. the unintentional insider threat). It is vital that organizations understand normal employee baseline behaviors and also ensure employees understand how they may be used as a conduit for others to obtain information. The following product is intended to act as a springboard for organizations to consider policies and practices used to detect and deter the insider threat.

The Insider

Building a baseline understanding of the personalities and behavioral norms of those previously defined as 'insiders' will make detecting deviations in these norms easier. Some general behavioral characteristics of insiders at risk of becoming a threat include:[2,3]

Characteristics of Insiders at Risk of Becoming a Threat	
Introversion	Minimizing their mistakes or faults
Greed/ financial need	Inability to assume responsibility for their actions
Vulnerability to blackmail	Intolerance of criticism
Compulsive and destructive behavior	Self-perceived value exceeds performance
Rebellious, passive aggressive	Lack of empathy
Ethical "flexibility"	Predisposition towards law enforcement
Reduced loyalty	Pattern of frustration and disappointment
Entitlement – narcissism (ego/self-image)	History of managing crises ineffectively

Individuals that exhibit these characteristics may reach a point at which they carry out malicious activity against the organization. One of the best prevention measures is to train employees to recognize and report behavioral indicators exhibited by peers or business partners.

Some Behavioral Indicators of Malicious Threat Activity:[4,5]

- *Remotely accesses the network while on vacation, sick or at odd times*
- *Works odd hours without authorization*
- *Notable enthusiasm for overtime, weekend or unusual work schedules*
- *Unnecessarily copies material, especially if it is proprietary or classified*
- *Interest in matters outside of the scope of their duties*
- *Signs of vulnerability, such as drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health or hostile behavior, should trigger concern. Be on the lookout for warning signs among employees such as the acquisition of unexpected wealth, unusual foreign travel, irregular work hours or unexpected absences*[6]

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:

Some Behavior Prediction Theories To Consider[7]	
General Deterrence Theory (GDT)[8]	Person commits crime if expected benefit outweighs cost of action
Social Bond Theory (SBT)[9]	Person commits crime if social bonds of attachment, commitment, involvement and belief are weak
Social Learning Theory (SLT)[10]	Person commits crime if associates with delinquent peers
Theory of Planned Behavior (TPB)[11]	Person's intention (attitude, subjective norms and perceived behavior control) towards crime key factor in predicting behavior
Situational Crime Prevention (SCP)[12]	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*).[13,14] Understanding these stages may help organizations put individual risk characteristics and behavioral indicators 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:[15]

- Training 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

Detect and Deter

It is worth noting that one recent study names local area network (LAN) access as the top vector for insider threats/misuse (71%), followed by physical (28%) then remote access (21%).[16] The following offers detection, prevention and deterrence methods to consider. Additional reference points have been added for convenience in the event organizations are interested in pursuing particular methods.[17]

Some Security Technologies to Detect/Prevent Insider Attacks Include:[18,19,20,21]	
Data/file encryption	Enterprise identity and access management (IAM)[22]
Data access monitoring	Data access control[23]
SIEM or other log analysis[24]	Intrusion detection/ prevention systems (IDS/IPS)
Data loss prevention (DLP)	Enterprise digital rights management solution
Data redaction	

Some Deterrence Methods Include:[25,26,27]

- *Deploy data-centric, not system centric security*
- *Crowd-source security*
- *Use positive social engineering*
- *Think like a marketer and less like and IDS analyst*
- *Build a baseline based on volume, velocity, frequency and amount based on hourly, weekly, and monthly normal patterns*
- *Use centralized logging to detect data exfiltration near insider termination*[28]
- *Require identification for all assets (e.g. access cards, passwords, inventory check out)*
- *Note frequent visits to sites that may indicate low productivity, job discontent and potential legal liabilities (e.g. hate sites, pornography)*
- *Announce the use of policies that monitor events like unusual network traffic spikes, volume of USB/mobile storage use, volume of off-hour printing activities and inappropriate use of encryption*[29]

- *Provide avenues for employees to vent concerns and frustrations to aid in mitigating the insider threat motivated by disgruntlement*
- *Implement employee recognition programs that offer public praise to aid in mitigating the insider threat motivated by ego*
- *Authorize users based on least access privilege and conduct periodic audits to detect inappropriately granted access or access that still exists from previous job roles/functions and should be removed*[30]

Training

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

- The Department of Homeland Security (DHS) offers an online independent study course titled Protecting Critical Infrastructure Against Insider Threats (IS-915).[31] The one-hour course provides 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 Threat Awareness Course[32] free of charge. 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.

Point of Contact

Please direct any questions or comments about this product to the NCCIC Analysis team at NCCIC@hq.dhs.gov.

Feedback

NCCIC/US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL:

https://www.us-cert.gov/forms/feedback

References

[1] https://www.cert.org/insider-threat/

[2] http://csrc.nist.gov/organizations/fissea/2012-conference/presentations/fissea-conference-2012_mahoutchian-and-gelles.pdf

[3] http://www.cis.aueb.gr/Publications/Security%20Project%202014.pdf

[4] http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

[5] http://csrc.nist.gov/organizations/fissea/2012-conference/presentations/fissea-conference-2012_mahoutchian-and-gelles.pdf

[6] http://www.thei3p.org/research/mitremi.html

[7] http://www.cis.aueb.gr/Publications/Security%20Project%202014.pdf

[8] http://www.ee.oulu.fi/~vassilis/courses/socialweb10F/reading_material/5/darcy08.pdf

[9] http://link.springer.com/chapter/10.1007/978-1-4419-7133-3_3

[10] http://sites.duke.edu/ihss/files/2011/12/CyberSecurityResearchBrief-Final_mcbride-2012.pdf

[11] Willison, R., & Warkentin, M. (2013). BEYOND DETERRENCE: AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE. *MIS Quarterly*, *37*(1), 1-20.

[12] http://www.palgrave-journals.com/sj/journal/v26/n4/abs/sj201325a.html

[13] http://www.ieee-security.org/TC/SPW2013/papers/data/5017a060.pdf

[14] http://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf

[15] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6758854

[16] Verizon Data Breach Investigations Report (DBIR, 2014)

[17] Software Engineering Institute (CERT), Common Sense Guide to Mitigating Insider Threats, 4th Edition, CMU/SEI-2012-TR-012

[18] http://www.vormetric.com/sites/default/files/ap_Vormetric-Insider_Threat_ESG_Research_Brief.pdf

[19] http://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf

[20] http://srg.cs.illinois.edu/srg/sites/default/files/forenscope-cae-wit_0.pdf

[21] http://www.afcea.org/events/augusta/13/documents/Track3Session4_RaytheonDefenseProgramsGovernmewntSolutionsLamarBC.pdf

[22] http://epub.uni-regensburg.de/15129/1/FuPe10.pdf

[23] http://www.morganclaypool.com/doi/abs/10.2200/S00431ED1V01Y201207DTM028

[24] http://www.aveksa.com/wp-content/uploads/2013/07/WP-SIEM-Deployments-Overview.pdf

[25] http://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf

[26] http://www.raytheon.com/capabilities/rtnwcm/groups/iis/documents/content/rtn_iis_whitepaper-investigati.pdf

[27] http://www.mitre.org/publications/project-stories/the-human-factor-using-behavioral-science-to-counter-insider-threats

[28] http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9875

[29] http://searchsecurity.techtarget.com/tip/Monitoring-strategies-for-insider-threat-detection

[30] http://www.ey.com/Publication/vwLUAssets/EY_-_Our_experience_will_enable_you_to_detect_and_respond_to_the/$FILE/EY-Authorized_access_uncovering_insider_threats_within_oil_and_gas_companies.pdf

[31] http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-915

[32] http://cdsetrain.dtic.mil/itawareness/