Categories of Insider Threats

SUMMARY

Currently, no uniform lexicon exists to characterize the different types of insider threats. Organizations, whether in the public or private sector, typically develop their own categories, which results in numerous related but dissimilar terms and definitions. This lack of a common lexicon creates confusion among security experts who study and develop strategies to mitigate insider threats. A consistent top level categorization of the broad range of insider threats would enable better sharing of best practices and lessons learned, thereby helping to mitigate risk.

BACKGROUND

While organizations may use terminology that uniquely "fits" their organization, by mapping their efforts to these standardized terms they will help facilitate information sharing and application of expertise.

- Categories of Insider Threats broadly classifies the nature of insider threats organizations face today with common terms that facilitate information-sharing and learning.
- More than 35 types of insider threats were reviewed. Although a variety of terms are used constructively by individual government agencies and companies, INSA's Insider Threat Subcommittee found that the most overarching and inclusive definitions were rooted in academic research.
- This effort to categorize insider threats naturally opens the door to further analysis and discussions on the subject. These sub-topics include:
  - Thresholds for understanding and categorizing the different types of insider threats.
  - Deeper analysis into the motives driving insider threat behaviors within these categories, including even sub-categories of these types of insider threats.
  - Critical pathways, precursor activities, and behaviors for these categories.
  - Unique environmental and organizational factors that lead to or enable insider threats, as well as mitigation options that may be specific to these categories.

CATEGORIES OF INSIDER THREATS

DEFINITION OF INSIDER THREAT

The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly or unwittingly, commits acts in contravention of law or policy that result in, or might result in, harm through the loss or degradation of government or company information, resources or capabilities; or who commits destructive acts, to include physical harm to others in the workplace.

TYPES OF INSIDER THREAT

Following are terms with greatest resonance and most widespread use:

SABOTAGE: An insider's destruction of electronic or physical property intended specifically to harm his/her own organization or an individual within the organization.[i]

THEFT OF INTELLECTUAL PROPERTY OR NATIONAL DEFENSE INFORMATION: An insider's theft of intellectual property, data, or classified information relevant to national security. This category encompasses the traditional concept of espionage as defined by applicable statutes.[i]

INSIDER FRAUD: Modification, addition, deletion, or inappropriate use of an organization's information, data, or systems for personal gain. Examples include insider trading, embezzlement, and other actions to defraud the organization by an employee, contractor or trusted business partner.[ii]

UNINTENTIONAL INSIDER THREAT: An insider who has or had authorized access to the organization's network, system, physical facility, or data and who, through action or inaction *without malicious intent,* causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity or availability of the organization's information or information systems.[i] Examples include accidental public disclosures of sensitive information, phishing scams, and loss of organizational records and/or electronic media.

WORKPLACE VIOLENCE: Any act or threat or act of physical violence, harassment, hazing, intimidation or other threatening disruptive behavior that occurs at a work site.[iii]

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to compile this list of insider threat categories.

INSA MEMBERS

Mike Hudson, *ClearForce LLC*

Sam Worth, *DITMAC*

Wai Woolsey, *Palo Alto Networks*

Cathy Albright, *Thomson Reuters Special Services*

Julie Ard, *Haystax Technology*

INSA STAFF

Chuck Alsup, *President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Policy & Communications Director*

Caroline Henry, *Marketing & Communications Assistant*

Megan Anderson, *Intern*

Jessica Willmore, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and its 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

www.INSAonline.org

ADDITIONAL RESOURCES

[i] *CERT Insider Threat Center, Common Sense Guide to Mitigating Insider Threats, 5th ed., Carnegie Mellon University Software Engineering Institute, Technical Note CMU/SEI-2015-TR-010, December 2016, p. 23. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.*

[ii] *Frank Greitzer, Justin Purl, YM Leong, D.E. Becker, SOFIT: Sociotechnical and Organizational Factors for Insider Threat. IEEE Symposium on Security & Privacy, Workshop on Research for Insider Threat (WRIT), San Francisco, CA, May 24th, 2018.https://www.ieee-security.org/TC/SPW2018/WRIT/WRIT%202018%20SOFIT%20Sociotechnical%20and%20Organizational%20Factors%20for%20Insider%20Threat.pdf.*

[iii] *Greitzer,et. al., 2018.*