NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

INSIDER THREAT (InTh)

THIS PRODUCT WAS PUBLISHED BY THE NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE AND THE NATIONAL INSIDER THREAT TASK FORCE

Social Media And Insider Threat Risk

National Insider Threat Awareness Month 2022, Bulletin 1

National Insider Threat Awareness Month is an opportunity for individuals, government agencies, and public and private sector entities to reflect on the risk that those with authorized access can present to the safety, security, and stability of an enterprise. This year's focus includes social media's influence in facilitating insider threat activity, and the need for critical thinking in digital spaces.

Social media, websites, and applications which allow users to create or share content are widespread and immensely popular. Surveys and studies suggest that a sizable majority of Americans use social media regularly. For many working adults, social media sites provide a means of staying in touch, sharing opinions, receiving news, being creative, learning new skills, and much more.

But for all its positive attributes, social media carries a variety of detrimental impacts, including: 1) online "echo chambers" that repeat conspiracy theories and misinformation, 2) users feeling varying degrees of social isolation, 3) increasing emotional issues related to things like body image, 4) bullying and harassment, and 5) privacy concerns. Additionally, international and domestic terror organizations have utilized online networks to recruit and influence individuals. Fringe and even mainstream social and political movements leverage social media to influence individuals regarding their ideas or platforms. The most popular social media sites sometimes facilitate the sharing of opinions no matter how unfiltered, uninformed, or irrational.

It is critically important that insider threat program staff, as well as all other personnel within an organization, are attuned to the ways in which social media may escalate risk. External influence and perceived pressure from social media can negatively impact the degree of insider threat risk within an organization. Here are some examples:

- In a rush to post a new installment on their daily feed, an employee inadvertently photographs sensitive information and equipment in the background of their selfie.
- Over a span of months, a contractor is drawn into an online political collective from which they derive all of their news and information – much of which is false. They soon become obsessed with the employer's supposed greed and rather than pursuing appropriate whistleblower or reporting channels, begin working to undermine the organization.
- A disgruntled employee begins to see their favorite social media platform, with its global reach and widespread use, as a means of becoming famous and to really "make a difference" by publishing classified information that most people would find "shocking".

Defending against insider threats and minimizing insider threat risk requires a multi-disciplinary approach that leverages (at a minimum) the legal, security, information technology, and human resource elements of an organization. Insider threat programs should be geared toward ***preventing*** insider threats, often through educating staff to social media risks in addition to all types of external threats. Early intervention with a troubled employee often results in a positive outcome for them and the organization.
For more information on National Insider Threat Month: National Insider Threat Awareness Month 2022 (cdse.edu), or the Insider Threat Mission: National Insider Threat Task Force (NITTF) (dni.gov)