BTAC BULLETIN

EMERGING ISSUES, TRENDS, CAPABILITIES, AND BEST PRACTICES IN INSIDER THREAT ANALYSIS

Unauthorized Disclosure

The ***unauthorized disclosure (UD)*** of critical information, through leaks, espionage, spills, and failed safeguarding, can greatly degrade national/organizational security[1], brand reputation, and corporate profitability. Studies[2,3] on incidents of *intentional* UD highlight intervention points, and provide insights in how organizations can prevent, detect and mitigate impacts of insider threat. Most individuals that perpetrate acts of UD do not enter the DoD with malintent, instead, they are insiders who, over time and in reaction to situations and stresses, progress on a critical pathway[4] towards a disclosure. Key statistics identify workplace conflicts around career status and the way managers address feedback and accountability as a point where positive action and leader engagement can move someone off the pathway to an intentional UD. Additional insights highlight that while our efforts to reduce electronic methods of UD and identify individuals with high levels of debt have been successful, most intentional UD perpetrators take physical copies out of facilities and when it comes to money, are motivated by greed and not debt. This nuance highlights the need for complex threat assessment of human behavior and the utilization of DoD insider threat capabilities to address UD motivations.

WHAT CAN WE DO?

To mitigate insider threat and UD

1. **GOOD MANAGEMENT IS UD PREVENTION:** Whether it's subordinates, co-workers, or service members, get to know the people around you, so you can identify indicators, changes in behavior and potential team conflict before they escalate.
2. **REPORT INCIDENTS TO INSIDER THREAT HUBS:** Let experts assess if someone is moving down the critical pathway. Ensure you document and report all concerning behaviors no matter the incident "size". If behavior is reported early, it may be possible to help someone back on the right path and save a career.
3. **SPECIALIZED TRAINING FOR STAFF AND LEADERS:** Invest in your staff. Train leaders, security personnel, and others involved with disciplinary notices on conflict resolution and de-escalation strategies[2].

CHARACTERISTICS OF INTENTIONAL UD[2]

ADJUDICATIVE GUIDELINES

Top 4 adjudicative guidelines that perpetrators demonstrated pre-arrest:

1. **Handling protected information**
2. **Personal conduct**
3. **Foreign preference**
4. **Foreign influence**

Adjudicative guidelines give us minimum reporting standards, but it's vital that the detection methods and focus go beyond these criteria.

THREAT INDICATORS

25%

25% of perpetrators leaked to a non-accomplice about their UD activities

24%

24% of perpetrators experienced an event related to work status (conflict, demotion, clearance suspension)

MOTIVATIONS

Top 4 Motives for engaging in intentional UD:

1. **Money (greed)**
2. **Ideology**
3. **Revenge**
4. **Career Improvement**

Adjudication guidelines identify debt load as an indicator, but it's important to understand that "greed" is a less easily detected, but more accurate factor in UD.

MITIGATING FACTORS

Persons, things, or circumstances of sufficient value to the individual that reduce the likelihood they may act upon malicious intent. When these stabilizers "evaporate" it becomes easier to progress down the critical path.

METHODOLOGY

The most common method of exfiltration was the physical removal of printed or copied documents from a facility hidden on the person or in their personal items out of the building. Technology makes up a small proportion of the successful intentional UD

1. Office of the Director of National Intelligence. (2017). ICD 701, Unauthorized Disclosures of Classified National Security Information. https://www.dni.gov/files/documents/ICD/ICD-701-Unauthorized-Disclosures-2017-10-03.pdf 2. PERSEREC, Jaros, S., Rhyner, K., McGrath, S., Gregory, E. (2019). The Resource Exfiltration Project: Findings from DoD Cases, 1985-20174. 3. Bruce, J., & Jameson, G. (2013) *Recommendations for Preventing and Deterring Unauthorized Disclosures in the Department off Defense,* RAND National Defense Research Institute 4. Shaw, E.D., & Sellers, L. (2015). Application of the Critical Path Method to Evaluate Insider Risk. Studies in Intelligence, 59, 1-8.

DITMAC DOD Insider Threat Management and Analysis Center

BTAC Contact // dcsa.quantico.dcsa.list.ditmac-sme@mail.mil