INSIDER THREAT DEFENSE GROUP

Security Behind The Firewall Is Our Business

DoD PERSERC Report - The Resource Exfiltration Project: Findings from DoD Cases (1985-2017)

Despite changes in policies and practices over the years, perpetrators continue to exfiltrate resources from DoD and transmit them to unauthorized recipients. In recognition of this persistent and evolving insider threat, the Defense Personnel and Security Research Center (PERSEREC) examined cases of resource exfiltration, or cases that involve the intentional and unauthorized removal of DoD resources from authorized locations, to identify potential intervention points along perpetrators' pathways to criminal behavior. The purpose of this project was to analyze the current state of resource exfiltration and provide operationally relevant, empirically based recommendations to DoD stakeholders in order to improve efforts to detect, prevent, and mitigate these insider threats.

The objective of this study was to identify common themes and behavioral indicators that preceded individuals' arrests in order to prevent and mitigate future incidents. In total, 83 cases of DoD resource exfiltration were included in this study, and researchers collected information related to 392 variables of interest, to include pre-arrest behavior that matched disqualifying factors of the Adjudicative Guidelines and/or behavioral threat assessment themes. Full Report

Highlights Of Report

Nearly all of the perpetrators were male. They varied by age, citizenship, marital status, parental status, and education. Most exfiltration careers lasted less than 2 years, and nearly all ended within 10 years.

To remove resources, perpetrators most often carried them out the door of a secure facility, usually concealed in an everyday object such as a bag or briefcase. Among those who transmitted material to a foreign entity, Russia was the most common recipient. The most common motive was money, followed by ideology.

Researchers broke down the 13 Adjudicative Guidelines into 75 disqualifying factors in order to identify pre-arrest behavioral indicators.

The 10 most common disqualifying factors clustered in four of the 13 Adjudicative Guidelines; Foreign Influence, Foreign Preference, Personal Conduct, Handling Protected Information. See Table 6: Page 22

In contrast, the least common disqualifying factors were Sexual Behavior, Financial Considerations, Alcohol Consumption, Drug Involvement, and Outside Activities.

Overall, 65 out of the 83 perpetrators (78%) exhibited behavior that corresponded with at least one of the 10 behavioral threat assessment variables. Notably, nearly one-quarter of all perpetrators talked about their exfiltration activities to someone who was neither a handler nor an accomplice, and in 32 out of the 83 cases, people noticed concerning behavior or changes in behavior prior to the perpetrators' arrests. See Table 7: Page 23

Disqualifying Factors For The Adjudicative Guidelines

Overall, perpetrators demonstrated pre-arrest behavior that corresponded with at least one disqualifying factor associated with all 13 Adjudicative Guidelines prior to their arrest. In fact, as shown in Figure 2, all 83 perpetrators (100%) engaged in some kind of behavior that corresponded with at least one of the disqualifying factors included in Guideline K: Handling Protected Information, with Guideline E: Personal Conduct close behind (n=82).

EXFILTRATION METHODS

Finding And Recommendations

Finding #1:

User activity monitoring enables DoD to observe the electronic movement of its resources, but there appears to be insufficient protections against unauthorized physical movement. In this study, 65 out of the 83 perpetrators "collected or stored classified or other protected information at home or in any other unauthorized location."

Of the 37 perpetrators for whom relevant open source intelligence was available, only 10 leveraged technology, such as email or fax, to move resources from an authorized to an unauthorized location. Instead, the majority physically walked resources out the door, either concealed on their bodies (i.e., pocket, under a hat) or in a container, such as a briefcase.

Recommendation #1:

Where possible, DoD should reduce the number of locations within a facility where critical electronic assets can be printed and/or physically reproduced. Then, DoD should institute random physical inspections, again when possible.

BEHAVIORAL INDICATORS

Finding #2:

The majority of perpetrators exhibited pre-arrest behavioral indicators, but the behavioral threat assessment framework appears to yield more actionable results than those indicators derived from the disqualifying factors associated with the Adjudicative Guidelines.

Although all 83 perpetrators (100%) engaged in some kind of behavior that corresponded with at least one of the 13 Adjudicative Guidelines, closer analysis revealed limited insight into potential intervention points prior to resource exfiltration. For example, 80 perpetrators "violated a written or recorded commitment made by the individual to the employer as a condition of employment." Similarly, 81 perpetrators "failed to comply with rules for the protection of classified or other protected information." Once a perpetrator has behaved in such a way that corresponds with either of these disqualifying factors, he / she likely has committed a serious crime associated with exfiltration, at which point it is likely too late to intervene.

In addition, some of the most commonly cited behavioral indicators for resource exfiltration appeared the least often among the perpetrators included in this study. For example, money was the most common motive, but the disqualifying factors associated with Adjudicative Guideline F: Financial Considerations yielded little to suggest the presence of financial pressures among the perpetrators. In other words, the financial motive did not appear to stem from debt but from greed.

In contrast with the Adjudicative Guidelines, experts designed the behavioral threat assessment framework specifically to identify and mitigate concerning behavior before it escalated. Sixty-five out of the 83 perpetrators exhibited behavior that corresponded with at least one of the 10 behavioral threat assessment variables included in this study. For example, nearly one-quarter of all perpetrators (n=21) talked specifically about their exfiltration activities to someone who was neither a handler nor an accomplice.

In 32 of the cases, someone noticed a change in behavior or concerning behavior prior to the perpetrator's arrest, and of those, 23 cases involved someone who witnessed something and went on to report what they saw.

Recommendation #2:
DoD should integrate best practices for behavioral threat assessment into the insider threat training mandated by the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs for both Insider Threat Program Personnel and the general workforce

PROFESSIONAL STRESSORS
Finding #3:
Employees who experience professional stressors, such as a demotion, could target DoD for retaliation against perceived wrongs. In this study, nearly one-quarter of all perpetrators experienced an issue or event related to their professional status that facilitated the decision to exfiltrate resources. Moreover, behind money and ideology, a desire for revenge and a desire to improve one's career were the most common motives for resource exfiltration. These results emphasize the importance for supervisors, commanders, and Human Resources personnel to respond to problematic behavior with care and consideration, so as not to endanger the future welfare of DoD or its resources.

Recommendation #3:
DoD should ensure that its personnel who issue disciplinary notices are trained in conflict resolution and / or de-escalation strategies, and security personnel should be on hand to ensure those who are terminated do not retain physical or logical access. DoD also should prioritize additional research to identify best practices to reintegrate employees into the workforce after serious disciplinary action, such as a demotion or suspension. Together with wellness programs such as Employee Assistance Programs, these practices should help to ensure employees successfully recover from difficult events and situations.

Please contact the ITDG to learn more about the Insider Threat Mitigation training courses or consulting services we offer.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program Development / Management Training Course Instructor
Insider Threat Vulnerability Assessor & Mitigation Specialist
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us
james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org