NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

OPERATIONS SECURITY (OPSEC)

THIS PRODUCT WAS PUBLISHED BY NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE & THE NATIONAL OPERATIONS SECURITY PROGRAM (NOP) OFFICE

Understanding OPSEC from an Organizational Perspective

National OPSEC Awareness Month, January 2023, Bulletin 4

National Operations Security (OPSEC) Awareness Month is an opportunity for individuals, government agencies, and private sector entities to reflect on ways to mitigate risks to their organizations. OPSEC is a systematic and proven process for denying adversaries access to information about an organization's capabilities and intentions. An OPSEC program should be codified within an organization and remain ongoing to adequately protect data that can be leveraged by those seeking to harm an organization.

The first step in establishing an OPSEC program is acknowledging that adversarial threats to the organization exist. Every organization faces potential adversarial threats, whether they come in the form of crime, foreign espionage, terrorism, or subversion. Ransomware delivered by cybercriminals, sabotage conducted by insiders, theft of intellectual property by agents of a foreign intelligence service, or physical destruction of facilities by foreign or domestic terrorists are all examples of threats that can be mitigated through OPSEC.

Once an organization accepts and identifies likely adversaries, it can work to limit the exposure of data that would benefit those adversaries, shore up vulnerabilities, and develop strategies to mitigate risks. When adversaries are able to gather sufficient unprotected information relating to an organization's operations, capabilities, and plans, they can combine that data to create a full picture of their target, identify vulnerabilities, and exploit the information to their advantage. Even a small competitive advantage over the organization could potentially result in loss of operating efficiency, adversely impact revenue or stock price, or in a worst-case scenario, pose physical harm to employees.

OPSEC practices help reduce the availability of data that adversaries can collect and use. OPSEC is an ongoing process; it is not "one and done." It requires repeated re-assessment of the equities at stake and their vulnerabilities, as well as the countermeasures to be developed and implemented. OPSEC also requires internal coordination among security elements within an organization, such as personnel security, physical security, insider threat, counterintelligence, cybersecurity, and information assurance. Other elements of the organization, such as human resources, acquisition, and logistics, should be engaged to identify critical information to be protected and vulnerabilities to be addressed.

OPSEC is a holistic effort to frustrate adversary efforts to leverage vulnerabilities to their advantage. As a bonus, the same OPSEC processes that protect large organizations can help individuals reduce their vulnerabilities. This reality can be useful in helping workforces embrace a security mindset, as research shows that organizations with a security "culture" are less likely to be victimized and suffer losses.

During National OPSEC Awareness Month, please take the opportunity to learn about OPSEC and understand its role in securing your organization and providing benefits to you personally.

The National OPSEC Program Office provides OPSEC resources and awareness materials year round. Please visit the following link: National Operations Security Program Office (NOP) (dni.gov)