Operational security

Psychology

Operations Security Provide an example of a law enforcement agency in the United s that has implemented effective operational security (OPSEC) procedures since 9/11?

Operations security (OPSEC) is a term that traces its origin from the jargons used in the US military. The operations security process seeks to analyze information and assess any form of potential threats (Tipton & Krause, 2003). Several law enforcement agencies have successfully adapted OPSEC procedures. The FBI has adapted the OPSEC procedures to supplement their security planning (Tipton & Krause, 2003). The FBI falls under Homeland Security, which was tasked to ensure nothing like 9/11 attacks happens in the United States again. The bureau has been effective in implementing OPSEC procedures to aid in threat assessment and detection.

What were the OPSEC procedures?

Operations security systems focus on fighting terrorism using proactive measures instead of reactive measures. The FBI has implemented all the steps, which has boosted the fighting against terrorism. The starting step in the OPSEC process is the identification of critical information that an enemy might need to attack. The identification of critical information aids in protecting the most important information. Second, an analysis of all the threats should be performed. Threat analysis entails research and comprehensive of intelligence, open source information and counterintelligence (Andress, 2011). They might help in determining the potential threats.

The third step in the operation security process is the analysis of vulnerabilities. It involves assessing the entire operation with the aim of identifying any OPSEC indicators that could reveal sensitive information. The

intelligence obtained at this stage is compared with what the enemy's intelligence is capable. Information on the capability of the enemy's intelligence was determined during threat analysis. Risk assessment is the next after analysis of vulnerabilities. The operation planners work around the clock to identify the vulnerabilities that have been identified. They come up with OPSEC measures to each identified vulnerability. OPSEC measures are selected for application. The final process in operations security is the application of relevant measures. The command is expected to implement the measures that were identified during risk assessment. It can also entail the implementation of OPSEC measures that are found in implementation plans.

Describe what problems you envision the lack of an effective OPSEC program could hold for a local, county, state, tribal, or federal law enforcement agency.

The lack of an efficient operation security program puts the law enforcement agencies at an enormous risk. Information and communication are critical factors when it comes to the effective functioning of any law enforcement agencies. As a result, terrorist tend to target communication networks that belong to law enforcement agencies. The aim is to ensure communication is impossible. The presence of an OPSEC would ensure that law enforcement agencies could protect their communication network.

Improper planning and inadequate analysis might lead to mistakes that cost lives. Operations security program ensures law enforcement officers are taught to analyze threats and come up with valid conclusions (Baker, 2005). Threat analysis is very importance since it gives a law enforcement agency a chance to be proactive. The program encourages proactive measures, which

are effective in preventing terrorist attacks. Reactive measures can lead to the manipulation of a security agency. The use of intelligence analysts helps in assessing a threat and determining the best solution. It would not be possible without the establishment of an OPSEC program. An OPSEC program ensures law enforcement agencies perform at their best whether it is local, state, county or federal level.

References

Andress, J. (2011). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Burlington: Elsevier Science.

Baker, T. E. (2005). Introductory Criminal Analysis. Pearson Custom Pub.

Tipton, H. F., & Krause, M. (2003). Information " Security Management Handbook. CRC Press.