technology solutions
that make business sense

5 Fundamentals of Operational Security

While operational security, or OPSEC, has its origins in securing information important to military operations, it has applications across the business community today.

In a commercial context, OPSEC is the process of denying hackers access to any information about the capabilities or intentions of a business by identifying, controlling and protecting evidence of the planning and execution of activities that are essential the success of operations.

OPSEC is a continuous process that consists of five distinct actions:

- Identify information that is critical to your business.
- Analyze the threat to that critical information.
- Analyze the vulnerabilities to your business that would allow a cyber criminal to access critical information.
- Assess the risk to your business if the vulnerabilities are exploited.
- Apply countermeasures to mitigate the risk factors.

In addition to being a five-step process, OPSEC is also a mind-set that all business employees should embrace. By educating oneself on OPSEC risks and methodologies, protecting sensitive information that is critical to the success of your business becomes second nature.

This section explains the OPSEC process and provides some general guidelines that are applicable to most businesses. An understanding of the following terms is required before the process can be explained:

- ***Critical information*** - Specific data about your business strategies and operations that are needed by cyber criminals to hamper or harm your business from successfully operating.
- ***OPSEC indicators*** - Business operations and publicly available information that can be interpreted or pieced together by a cyber criminal to derive critical information.
- ***OPSEC vulnerability*** - A condition in which business operations provide OPSEC indicators that may be

Cyber Plan Action Items:

01 Identity of critical information.

The identification of critical information is important in that it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all information relevant to business operations. Given that any business has limited time, personnel and money for developing secure business practices, it is essential to focus those limited resources on protecting information that is most critical to successful business operations. Examples of critical information include, but should not be limited to, the following:

- Customer lists and contact information
- Contracts
- Patents and intellectual property
- Leases and deeds
- Policy manuals
- Articles of incorporation
- Corporate papers
- Laboratory notebooks
- Audio tapes
- Video tapes
- Photographs and slides
- Strategic plans and board meeting minutes

02 Analyze threats.

This action involves research and analysis to identify likely cyber criminals who may attempt to obtain critical information regarding your company's operations. OPSEC planners in your business should answer the following critical information questions:

- Who might be the cyber criminal (e.g. competitors, politically motivated hackers, etc.)?
- What are the cyber criminal's goal?
- What actions might be the cyber criminal take?
- What critical information does the cyber criminal already have on your company's operations? (e.i., what is already publicly available)?

03 Analyze vulnerabilities.

The purpose of this action is to identify the vulnerabilities in your business of protecting critical information. It requires examining each aspect of security that seeks to protect your critical information and then comparing those indicators with the threats identified in the previous step. Common vulnerabilities for small businesses can include the following:

- Poorly secured mobile devices that have access to critical information
- Lack of policy on what information and networked equipment can be taken home from work or taken abroad on travel
- Storage of critical information on personal email accounts or other non-company networks.
- Lack of policy on what business information can be posted or accessed by social network sites.

04 Assess risk.

This action has two components. First, OPSEC managers must analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures to mitigate each one. Second, OPSEC measures must be selected for execution based upon a risk assessment done by your company's senior leadership. Risk assessment requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on business operations resulting from the exploitation of a particular vulnerability.

OPSEC measures may entail some cost in time, resources, personnel or interference with normal operations. If the cost to achieve OPSEC protection exceeds the cost of the harm that an intruder could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires your company's leadership approval.

05 Apply appropriate OPSEC measures.

In this action, your company's leadership reviews and implements the OPSEC measures selected in assessment of risk action. Before OPSEC measures can be selected, security objectives and critical information must be known, indicators identified and vulnerabilities assessed.

Helpful Links

The resources provide additional information in the origins, purpose and implementation of operational security.

- National Security Agency/ Central Security Service, PURPLE DRAGON. The origin and Development of the United States OPSEC Program (1993)
  http://www.nsa.gov/public_info/_files/crytologic_quarterly/purple_dragon.pdf
- Joint publication 3-13.3, Operations Security (29 June 2006): Available through Joint Doctrine Education and Training Electronic Information System (JDEIS).
  https://jfse.ndu.edu/schools_programs/jc2ios/io/student_reading/IC2_JP_3-13-3_OPSEC.Process,pdf
- National OPSEC Program:
  https://www.iad.gov/ioss/
- OPSEC Professional Society:
  http://opsecsociety.org/
- Operations Security Professional's Association:
  http://opsecprofessionals.org/
- Department of Homeland Security Critical Infrastructure Protection:
  http://www.dhs.gov/criticalinfrastructure