TELEDYNE BROWN ENGINEERING

2021 ANNUAL OPSEC AWARENESS BRIEFING

TELEDYNE
BROWN ENGINEERING
Everywhereyoulook™

OPSEC HISTORY

The Original Purple Dragon Survey Team

Coat of Arms

The original Purple Dragon Survey Team designed and developed a countermeasure program: methods and procedures for operations security problems they discovered during specific operations in Vietnam, that resulted in a raising of combat effectiveness, and the saving of human lives and material resources of an incalculable magnitude.

Their methodology was adopted by the federal government in 1988 as mandated by National Security Decision Directive Number 298 issued by President Ronald Reagan.

OPSEC

"… A systematic, proven process by which a government, organization, or individual can identify, control and protect generally unclassified information about an operation/activity and, thus, deny or mitigate an adversary's/ competitor's ability to compromise or interrupt said operation/activity."

NSDD 298 – National Operations Security Program

OPSEC PROCESS

- **Analyze the Threat**
- **Identify Critical Information**
- **Identify Indicators/Analyze Vulnerabilities**
- **Perform Risk Analysis**
- **Develop OPSEC Measures**

ANALYZE THE THREAT

Our Adversaries = The THREAT

- **What makes a Threat a Threat?**
  - Possess the Capability to collect, process and use knowledge of our activities against us via some type of action
  - And the Intent to carry out this

Common Adversaries:

- **Foreign Countries**
- **Terrorist Groups – Foreign and Domestic**
- **Corporate Competitors – Foreign and Domestic**

IDENTIFY CRITICAL INFORMATION

Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

IDENTIFY OPSEC INDICATORS

Indicators are derived from openly available information that adversaries can piece together or detectable activities that adversaries can interpret to reach conclusions or estimates concerning our mission and our critical information.

CRITICAL INFORMATION NODES

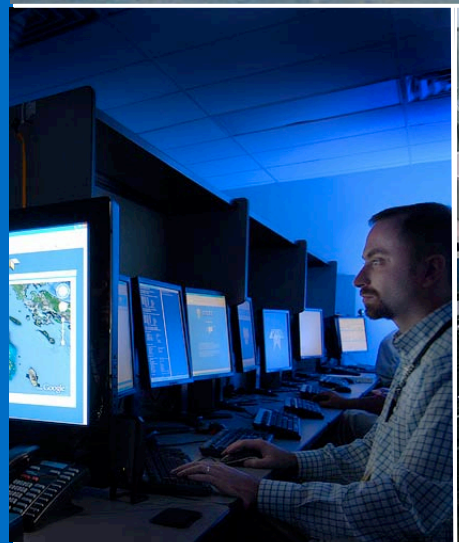
- Planning
- Operations
- Logistics
- Finance
- Public Affairs
- Travel
- Testing
- Communications
- Procurement
- Administration
- Contracts

ANALYZE VULNERABILITIES

An OPSEC vulnerability exists when :

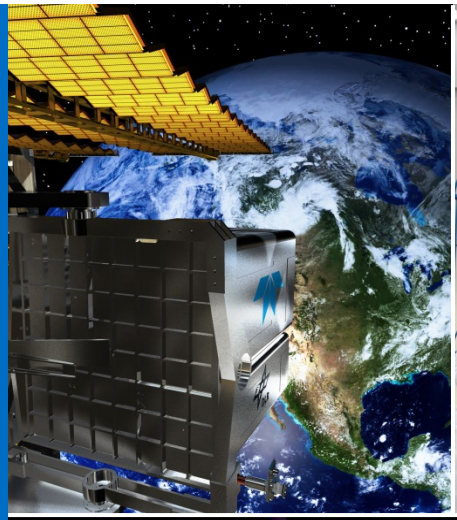
- **The adversary is capable of collecting critical information or indicators, analyzing it, and then acting quickly enough to impact friendly objectives.**

- **Conducting exercises, red teaming, and analyzing operations can help identify vulnerabilities.**



PERFORM RISK ANALYSIS

- The process of evaluating the risks to information based on susceptibility to intelligence collection.
- It involves assessing the adversary's ability to exploit vulnerabilities that would lead to the exposure of critical information and the potential impact it would have on the mission.



DEVELOP OPSEC MEASURES

Effective OPSEC Measures are usually simple changes of, or placing more emphasis on, security and/or operational procedures.

OPSEC Measures eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

PROTECT THE MISSION

- Do not “talk around” classified information.
- Be familiar with the sensitivity of the information you handle.
- Use appropriate security handling to protect critical information.
- Use appropriate Burn Bags for all information.
- Do not discuss official business in public places.
- Bring any OPSEC concerns to the attention of the appropriate personnel.
- Comply with OPSEC guidelines and recommendations.
- Review and minimize personal data on social networking web sites/pages.

ADVERSARIES COLLECT 24/7

Our adversaries don't keep business hours;

The gathering of information on our operations and capabilities is 24/7.

No weekends.

No holidays.

No vacations.

Our adversaries won't limit their activities to just our workplace.

They're in our neighborhoods.

They frequent the places we like to go.

They travel with us.

And they're on the Internet.

Monitored Information:

- Social Networking Sites – Facebook, LinkedIn
- E-mail – official and unofficial (UNCLASS and commercial)
- Official Websites/Associations/ Hobbies
- Cell Phones

ADVERSARIES COLLECT 24/7

OPSEC And Social Networking Sites-

Social networking sites are software applications that connect people and information in spontaneous, interactive ways. While fun, they can provide adversaries with potentially useful information that they could use against you and your family. Your information could end up in the public domain at any time due to hacking, configuration errors and social engineering.

Protect Yourself!

- **Teach your family the basics of Home Computer Security.**
- **Protect yourself from identity theft.**
- **Prepare yourself and your family for future emergencies.**

ACKNOWLEDGEMENT AND SUBMISSION

Please verify your acknowledgement of the 2021 OPSEC Annual Refresher Briefing below by entering your name and submitting via e-mail.

Thank you,

TBE Security

I have read and understand the content of the 2021 OPSEC training. I access, discuss, or hear classified information as part of my job function.

Signature

Gregg Legarda

Submit