Introduction

This OPSEC Presentation was developed by OSPA and is intended as an overview of the concepts and applications of OPSEC. This is NOT a presentation on “Military” OPSEC, nor “Civilian” OPSEC or any other specific application, but a demonstration that OSPEC can be applied in any environment due to the universal concepts and portability of the discipline.

The world is changing- getting smaller. Corporations, civilians and the government work together as never before. OPSEC can keep up.

Christopher R. Cox, OSPA, President
Module 1:

Introduction to OPSEC

Operations Security - What it is and isn’t

OSPA (www.opsecprofessionals.org)
OPSEC:

"Operations Security (OPSEC) is an analytic process used to deny an adversary information - generally unclassified - concerning friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations. OPSEC does not replace other security disciplines – it supplements them."
In other words…

OPSEC helps you control information that could be used against you.

OPSEC can be used to increase safety and security in ANY setting and for ANY purpose.
OPSEC is:

• A process that helps you examine your day-to-day activities from an adversary’s point of view
• A tool that helps you understand what an adversary can learn about your organization from your activities.
• A risk assessment tool
OPSEC is:

• A way to identify security risks and countermeasures
• A method that can be adapted to any operation, program, event or situation
• A cost-effective addition to your security arsenal
• A mindset, a way of life!
OPSEC is not:

• A strict set of “rules” and “procedures”
• An expensive and time-consuming process- OPSEC can be low-cost or free
• A process that is only used by the Government or Military. OPSEC can be used by corporations, schools, communities and individuals.
Consider some of the following “traditional” security programs:

- Personnel Security
- Physical Security
- Communications Security
- Information Security

Compliance is normally enforced through other procedures and processes…

…where OPSEC is a method and a process that can be practiced without memorizing a single “rule”!
OPSEC can be a **FORMALIZED**, structured program with its own staffing and support,

Or, OPSEC can be an **INFORMAL** and “fun” addition to your overall security program.

Or anything in between. Whatever works for YOUR organization.
When can OPSEC be used?

- Planning and Forecasts
- Planning for Special Events
- Special Training Exercises
- Plans and Standard Operating Procedures
- Methods, Sources, and Technical Tradecraft
- At home and on vacation
- To supplement existing security procedures
- Contracts/Bidding Processes
- Software and Source Code
- New designs, technical drawings, blueprints
And, OPSEC Supplements all of your other Security Programs!
Conclusion

OPSEC is an adaptable tool and method that can be applied to any situation and any organization or individual. It can be a formal program, or an addition to your security program. As long as it’s there! The more “OPSEC” you have, the stronger your security posture.
Module 2: OPSEC and You

How OPSEC affects the individuals, and the role they play.

OSPA (www.opsecprofessionals.org)
THE MOST IMPORTANT SECURITY TOOL IN OPSEC…

…IS FOUND IN THE MIRROR.
No matter your position, title or job, YOU have a part to play in OPSEC.
Every Person Is An OPSEC Sensor!

Every person in your neighborhood, company or organization is able to be a part of the security solution by:

✓ Knowing the threats
✓ Knowing what to protect
✓ Knowing how to protect it!
...And it’s mostly the front line individual that’s targeted,
And it’s the front line individual that’s better able to detect potential compromises.
A cat burglar is captured due to good OPSEC
Conclusion

Every person involved, and even family members, should be considered a part of the overall security program.

Every one of us can detect and help avert a threat. No matter your role, rank or position, you’re important in OPSEC!
Module 3: The OPSEC Process

OPSEC in five steps (and also in two!)

OSPA (www.opsecprofessionals.org)
The OPSEC “5-step Process” is more accurately described as a continual cycle of identification, analysis and remediation.
Definition: “Adversary”
(AKA- “Bad Guy”)

An adversary is anyone who **contends** with, **opposes** or **acts against** your interest and must be denied critical information.

It could be as simple and obvious as your opponent in any game, or as complex and unknown as a spy, agent of a foreign government, or a criminal.

Remember that each adversary will have its own **motivations** and **capabilities**

Examples include:

- Terrorist groups, foreign and domestic
- Criminals
- Organized crime groups
- Extremists
- Foreign Intelligence Services
- Hackers/Crackers
- Insider Threats
Definition: “Vulnerability”  
(AKA- “Weakness”)

A vulnerability is a weakness that can be exploited by an adversary to obtain your critical information, and it can be present in any facet of your operations.

Vulnerabilities can come from many sources in your operation to include the physical environment of the work area, the office operating procedures, computers, or a myriad of other sources.

A vulnerability is weakness that can be exploited by an adversary if it is discovered. A vulnerability exists when critical information is susceptible to exploitation by an adversary.

Potential Categories:
• Communications
• Public Affairs Department
• Critiques and after action reports
• Mail
• Trash
• E-mail
Definition: “Indicator”  
(AKA- “Clue”)

An indicator is a piece of **information** or an **activity** that can be **observed** and **combined** with other information to reveal sensitive information. An indicator acts as a “clue” to reveal information about an activity and will be the subject of analysis.

Examples of indicators:
- Increased training
- Unusual deliveries
- Advanced parties
- An increase in related personnel actions, such as TDY/business travel, financial preparation, etc.
- Large and frequent meetings
- Increased overtime
- Press releases and news items
Definition: “Threat”

“Threat” refers to the combination of an adversary and their intentions to undertake actions detrimental to friendly activities or operations. A threat can be thought of any potential danger that a vulnerability will be exploited by a threat agent.

Both intent AND capability must exist to be considered a threat.

Ask yourself:
“Does this person/group want to cause me/us harm?”
And, if so:
“Are they able to do so?”
Definition: “Risk” and “Impact”

“Risk” is the **probability** that an adversary will **compromise** your critical information.

“Impact” is the **effect** that this compromise would have on your organization. Impact is the “what would it mean” factor.
A “Countermeasure” is ANYTHING that can **reduce** or **negate** an adversary’s ability to exploit a vulnerability.

In other words, it’s whatever works to lower risk to an acceptable level.

For example:

- Changing your routine and routes
- Altering your schedule
- Varying routes for company-marked vehicles
- Using encryption/VPN
- Using unmarked cars when travelling in foreign countries
- When on vacation, having a trusted friend take in your mail and newspapers, turn on lights, etc
- Training employees to avoid discussing personal/company information in public
The OPSEC Process

Officially, there are five steps in the OPSEC process:

1. Identify Critical Information
2. Analyze the Threat
3. Analyze Vulnerabilities
4. Assess Risk
5. Apply Countermeasures
Step 1:
Identify Critical Information

The first step in the OPSEC Process is to identify critical information.

You need to know what you need to protect if you expect to be able to protect it!

In this step, critical information is identified by determining which information is critical to operations or desired by an adversary.
Step 2: Analyze the Threat

The more we know about an adversary’s capability, the better you can judge how and why they may collect the information that they need.

To analyze a threat, determine the following

- *Who is a potential adversary to your mission, operations or activity*
- *What the adversary already knows.*
- *What the adversary needs to know to be successful.*
- *What the adversary’s intent and capabilities are.*
- *Where the adversary is likely to look to obtain the information.*
Consider the following…

<table>
<thead>
<tr>
<th>Who is the adversary?</th>
<th>What is their intent?</th>
<th>Proven</th>
<th>Estimated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is their collection capability?</th>
<th>Proven</th>
<th>Estimated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In person</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Images/video</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(MASINT)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is the adversary capable of applying this collection ability to action against us?</th>
<th>Proven</th>
<th>Estimated</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Name a friend of the adversary:

<table>
<thead>
<tr>
<th>What are the friends’ collection capabilities?</th>
<th>Proven</th>
<th>Estimated</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGINT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HUMINT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMINT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(MASINT)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Will they share information with the adversary?</th>
<th>Proven</th>
<th>Estimated</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is this friends’ overall threat level?</th>
<th>Proven</th>
<th>Estimated</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGINT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HUMINT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMINT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(MASINT)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You should know this information for EACH adversary!
Step 3: Analyze Vulnerabilities

First, take a hard look at your organization. What are your vulnerabilities? How can they be exploited? In this step, don’t worry about likelihood or impact—consider any vulnerability, big or small.

Consider the following common vulnerabilities:

- **Newspapers piling up could tell a burglar when to break into a home**
- **Untrained employees can reveal critical information while talking on the phone or in public**
- **Poor document control/unsecured dumpsters could allow for technical drawings, company memos and planning notes, spreadsheets, working documents to fall into the wrong hands**
- **Untrained employees can reveal sensitive information in online forums or chat rooms**
- **Predictable patterns, when changed, can reveal the occurrence of a significant event**
Step 4: Assess Risk

Step 4 is the “decision time” step. When assessing risk, the analyst will decide if a countermeasure needs to be assigned to a vulnerability based on the level of risk it poses to the mission, operation or activity.

Many things are taken into account at this point, including the likelihood that the vulnerability will be exploited, the impact if successfully exploited and cost to apply the countermeasure.

Given the two situations, which would be the most beneficial to consider for countermeasure application?

1. The location of the customer waiting room allows customers to overhear some minor, local budget discussions if the meeting room door is left open. Redesign would cost $25,000.

2. Employees have information that could, if released, severely impact the company’s ability to function. They have not yet been trained to avoid discussing this information over unsecured medium. Training would cost $125 per employee for 10 employees.
RISK = THREAT x VULNERABILITY x IMPACT

If there is no threat, vulnerability OR impact, there is NO risk.
Step 5: Apply Countermeasures

This is the “action” step. To the greatest extent possible, starting with the highest risk vulnerabilities, countermeasures are assigned in order to lower or eliminate the risks.

It’s a one to one relationship- identify a high-risk vulnerability, and determine which countermeasure can mitigate it. Frequently, it’s a combination of low-cost countermeasures that afford the best security.

For example:

- **Letting your newspapers and mail pile up at home while on vacation can be mitigated by having a trusted friend collect them**
- **The possibility of sensitive material being found in refuse bins can be mitigated by implementing a “shred all” policy.**
- **The possibility of releasing critical information online can be mitigated through user training and policy**
- **The “waiting room” scenario in step 4 could be mitigated by closing the door or using a random noise noise generator**
REMEMBER:
The 5 steps can be performed in ANY ORDER to allow flexibility to the OPSEC’er.
The “OPSEC Two-Step”
In its most basic form, and suitable for every employee, user and person, OPSEC can be broken down into two steps:

1. Know what needs to be protected!
2. Know how to protect it!
REMEMBER

It is the responsibility of the security professional to answer those questions for the end-users

It is the responsibility of the end-users to do it!
Conclusion

OPSEC is what you make of it. You can use the concepts of OPSEC to allow you to see security from a different perspective, or you can follow the 5 (or 2) step process periodically to evaluate your security level.

It’s up to you- 2 steps, 5 steps, or a few good ideas.
Module 4:

“The Eyes of the Wolf”

Your organization from an adversary’s perspective

OSPA (www.opsecprofessionals.org)
“The strength of OPSEC is that it teaches you to see yourself from the eyes of your adversary...

...To evaluate from the eyes of the wolf.”

-OSPA
OPSEC as a mindset

In addition to being a process, OPSEC is also a mindset.

It means being able to consider your organization or environment from the point of view of your adversary.

This allows you to consider your vulnerabilities from the perspective of the threat based on their capabilities and actions.
For example-
Pretend for a second that you’re able to swap places with one of your adversaries.
Now look at your organization through THEIR eyes, based on what you’ve researched and learned about them.
Ask yourself, as your adversary:

• “What do I need to know?”
• “How can I learn it?”
• “Can I get in the building/area?”
• “Can I exploit anyone that can?”
• “Can I find the information somewhere else, like online?”
• “What can I learn from watching and observing?”
OPSEC is unique, because it’s most effective when seen from the perspective of an adversary.

If you don’t know the adversary, how will you know what they’re targeting? If you don’t know their target, how will you know what to protect?
Conclusion

“So it is said that if you know your enemies and know yourself, you can win a thousand battles without a single loss. If you only know yourself, but not your opponent, you may win or may lose. If you know neither yourself nor your enemy, you will always endanger yourself.”
-Sun Tzu, The Art of War

Know your adversary… Know what they want… Know how they may try to obtain it…Know how to protect it.
Module 5:

“Open Source Intelligence”

Hiding in plain site

OSPA (www.opsecprofessionals.org)
Definition: Open Source Intelligence

AKA- One of the greatest threats to any organization

1. Publically available information that any member of the public may lawfully obtain by my request or observation.
2. Unclassified information that has limited public information or access

Source: re-configure.org
According to some estimates, 90%-95% of usable intelligence can be collected from open sources that is not classified and not protected.

This alleged Al Qaeda training manual was captured in a raid by coalition forces in 2003. According to the material, the Al Qaeda estimates that 80%-85% of intelligence can be gathered online. For that reason, the same manual recommends using encryption and ciphers to hide information.
The enemy is watching…

In this digital world, there are very few truly “primitive” enemies. The enemy is:

Watching chatrooms

Following Twitters

Sending social engineering email (“phishing”)

Monitoring Forums

Connecting on Social Media

Listening
And they have the same tools at their disposal that our forces use:
But Open Source Intelligence existed before the internet made it “easy”, and the same techniques that were used decades ago still apply today.

- Newsletters
- Newspapers
- Building permits
- Credit reports
- Justifications
- Patent offices
- Funding info
- Discarded memos (when refuse bins are on public property, depending on local law)
- Phone books
- Press releases
- Trade publications
New technologies have made it possible to conduct Open Source Intelligence without leaving the computer:

- Google
- Facebook
- Craigslist
- Myspace
- Blogs
- Webpages
- Online people Searches
- BitTorrent
- Online news
- Twitter
- AIM/ICQ/Yahoo chat
- Online maps
- Online patent searches
- ‘Deep web’ searches
Consider your footprint…

Where would you find information about your mission, organization? Have you issued press releases? Do your employees have personal blogs? Is there information in Google News? Is there a regular newsletter that’s publically available?

Everywhere that information exists about your organization can be a possible piece of the puzzle.
“It” never goes away!

When you put information on the net, via your blog, MySpace, email, etc., you have to assume that it’s going to stay there forever.

Same thing with newspapers, magazines, and other media.

The only safe bet is to make sure that it never gets there in the first place!
For Example:

The “Internet Wayback Machine” takes periodic “snapshots” of website content.
1,524 saved “snapshots” for UN.org, with saved content and information
“BlackWidow” downloads all pages and files from a website, which can reveal pages and entries not meant to be publically accessible.
Back to basics

Just like in the OPSEC process, consider your **vulnerabilities** and **threats**:

<table>
<thead>
<tr>
<th>VULNERABILITY</th>
<th>THREAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Earth can reveal physical layouts and security postures</td>
<td>A potential adversary may gather information from Google Earth prior to attempting an intrusion</td>
</tr>
<tr>
<td>Search Engines may archive old versions of information or information not intended for release</td>
<td>Information, although recently changed or corrected, may still be in the Search Engine cache, or the Search Engine may find information not intended for release but stored on the server</td>
</tr>
<tr>
<td>Employee directories may outline structure and contact information</td>
<td>This information may enable potential attackers to better target information-gathering attempts</td>
</tr>
</tbody>
</table>
Back to basics, cont.

<table>
<thead>
<tr>
<th>VULNERABILITY</th>
<th>THREAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal or company-sanctioned blogs or websites may reveal information about</td>
<td>A competitor or other adversary may be able to obtain information about new technologies or previously unknown vulnerabilities</td>
</tr>
<tr>
<td>upcoming plans or existing vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Press-releases may reveal too much information about upcoming or current</td>
<td>A competitor or other adversary may use this information to make education assumptions about future activities.</td>
</tr>
<tr>
<td>projects</td>
<td></td>
</tr>
<tr>
<td>Trade and internal reports may reveal procedural or technical information</td>
<td>Example: AT&amp;T released information about trunk line frequencies that allowed certain individuals to make free calls</td>
</tr>
<tr>
<td>What else? Who should know?</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

When you put information on the internet (to include chats, file sharing, etc), assume that it’s going to be there forever.

You can never be sure here, once released, the information will go.

The important part is to make sure that critical information is not released in the first place!
Module 6: 

“Real World Examples”

OPSEC in Real Life

OSPA (www.opsecprofessionals.org)
OPSEC is a tool, procedure and mindset that can apply to many real-world scenarios in multiple environments. The following slides will present some of these historical and current examples.

“On paper” versus “Real World”
"Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion."

- George Washington

“If I am able to determine the enemy’s dispositions while at the same time I conceal my own, then I can concentrate and he must divide.”

- Sun Tzu
"...Don't forget, you men don't know that I'm here. No mention of that fact is to be made in any letters. The world is not supposed to know what happened to me. I'm not supposed to be commanding this Army.

- George Patton
April, 2008-

Two sets of confidential blueprints for the planned Freedom Tower, built on the site of the World Trade Center in New York. The detailed, floor-by-floor schematics were marked “Secure Document- Confidential” on each of the 300 pages. 14 pages were not recovered.
May, 2009-

The launch procedures for the Terminal High Altitude Area Defense (THAAD) ground-to-air missile defense system, used to knock down incoming Scud missiles in Iraq, were found on a second-hand, computer hard disk drive purchased on eBay.
Important Note:

The following examples and scenarios are not hard and fast rules—just possible scenarios.
Which family is most likely on vacation?

Hint: A buildup of newspapers and mail, a missing vehicle that’s normally present, and the absence of lights can all indicate that “no one’s home”.
A Note on “Mail Holds” and “News Holds”

“Conventional Wisdom” dictates that one should have their mail held by the post office, or their newspapers held by the delivery service. This is a good way to remove a potential indicator. But remember- when you put your mail or news on hold, that’s one more person that knows you’re on vacation, and they may not “get” OPSEC. Consider a friend or relative instead.
Which company may have an important event coming up? Or had a recent incident?

Hint: Parking lots are often easily observed, and patterns can be observed, allowing one to observe changes to the pattern.
Which unit may be preparing to deploy?

Hint: sudden and sizable deliveries may indicate upcoming activity. Free time may indicate the absence of upcoming deployment.
Conclusion

OSPA (www.opsecprofessionals.org)
What we’ve learned

• What OPSEC is
• How and why it’s used
• The OPSEC process (5 and 2 step)
• Open Source Intelligence
• How OPSEC affects us all

OPSEC is a life and livelihood saver that WILL, in all cases, increase your security.
OPSEC and Other Disciplines

OPSEC can be integrated with any other discipline and increase its effectiveness. For instance, OPSEC can be applied to computer security by helping to eliminate information that would assist hackers. Also, OPSEC can be applied to physical security by eliminating patterns in guard patrols and responses. OPSEC WILL increase your security.
"It's not that I see more than you – it's that I know what I see."

-Sherlock Holmes