OPSEC: Convincing? Or Confusing?
A Pragmatic Program Primer for Practitioners
by
Kurt Haase, OCP

PREFACE. As Wayne Morris, OCP, stated in his article Creating an OPSEC Culture (*The OPSEC Journal*, Fourth Edition, 1998) "For most of us, OPSEC is a part-time responsibility. But we would be remiss if we fail to target the rank-and-file within our organization...for it is they who are the conduit for a visible, dynamic, and provocative OPSEC Program. One of the dilemmas facing the OPSEC practitioner is how to reach the employee population and educate them on a topic that few truly understand and even fewer are acutely interested in. OPSEC briefings rarely play to standing-room-only audiences, but regulations and world events mandate us to educate people on threats, vulnerabilities, and countermeasures." Wayne further stated that "An OPSEC awareness program is a living program that must adapt and flex to the needs of the organization and the changing climate..."

I have particular regard for his last statement...OPSEC is a living program that must adapt and flex...to the changing climate. However, as an OPSEC practitioner I believe that we have an equal responsibility to employees, and not just to the organization. Employees make up an organization, and what affects them affects the organization (and vice versa). Hence this article, written with a threefold purpose:

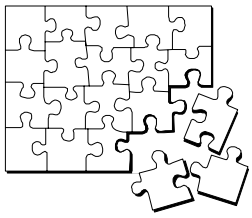
- First, if you are still "confused" about "OPSEC" – what it is and the role it plays -- this article will begin by presenting the basics of OPSEC in a unique adaptation. The remainder of the article will then demonstrate the application of the OPSEC process.

- Second, to provide you with an alternative approach to creating an OPSEC mind-set within your organization. Generally, employees "buy into" a program not because it is mandated but, rather, when they begin to realize "what it is and what it will do." This buy-in is also enhanced when they begin to understand how it will benefit them personally, and that, in reality, they have already been practicing OPSEC.

- Third, and what I consider to be the essence of this article, to take OPSEC to the "personal level" by describing an insidious threat to employees, their family, friends, co-workers, virtually everyone they know. The threat is called "identity theft." The compromise of their personal identity could place them in jeopardy of losing everything that they have worked and saved for. This threat has no organizational boundary; it matters not if they are a government agency employee, in the military, or a civilian contractor employee. In fulfilling this purpose, the threat will be presented, critical information will be identified, how personal information can be compromised (vulnerabilities) and how, by "securing against the inadvertent release of (critical) information" (i.e., applying countermeasures), the likelihood of becoming a victim could be reduced.

About the author. Kurt has been the OPSEC Program Manager for the Department of Energy, Nevada Operations Office (DOE/NV), Las Vegas, Nevada, since 1988. He has a B.S. and an M.A. in Police Science and Administration, is a member of the OPSEC Professionals Society, and an OPSEC Certified Professional (OCP). Kurt was the recipient of the National OPSEC Individual Achievement Award in 1994, and accepted the National OPSEC Organization Award in 1997 on behalf of DOE/NV. DOE/NV also received the National OPSEC Multi-Media Award in 1996, 1997, and in 1999.

Beginning with the Basics



Intelligence collection-and-analysis is very much like assembling a "picture puzzle." Each piece of the puzzle could be an item of information that is not classified or sensitive by itself but, when assembled with other "pieces of the puzzle," could damage national security by revealing classified or sensitive unclassified information regarding programs, activities, capabilities, intentions, vulnerabilities, or technology.

Concerns over the inadvertent release of sensitive information (i.e., the "pieces of the puzzle") led then President Reagan to sign *National Security Decision Directive 298* (NSDD298), Operations Security, mandating that all government agencies, departments, and their supporting contractors -- involved in National Security missions -- to establish an OPSEC program.*

NSDD 298 identifies the OPSEC methodology as a **five-step process**:

- **Y** Identify Critical Information
- **Y** Analyze the Threat
- **Y** Identify Vulnerabilities
- **Y** Assess the Risk
- **Y** Implement Appropriate Countermeasures

Changing the Approach to Understanding OPSEC

Anyone who has ever conducted an OPSEC briefing only to be met with "It's just another security program." or "But we already have a counterintelligence program." will understand the necessity of presenting OPSEC with a novel approach.

The first approach is to ensure that everyone understands what OPSEC is not. OPSEC is NOT a counterintelligence program, it is a countermeasures program. The difference is that counterintelligence is concerned with the intentional disclosure of classified information (generally for some form of personal gain), whereas OPSEC is concerned with the inadvertent disclosure of classified -- as well as sensitive unclassified -- information. In the event that classified information is intentionally released, then various statutes, Executive Orders, and regulations apply, not NSDD298.

Simply put, the role of OPSEC is to protect our critical and sensitive information from inadvertent compromise.

---

*Author's Note. Many articles have been written about the origin of OPSEC; why we -- as government or government-contractor employees -- should protect sensitive information; threats to our sensitive information; the costs associated with the loss of sensitive information; as well as the five-step process. Excellent sources of additional information and articles are the Interagency OPSEC Support Staff (IOSS, 6411 Ivy Lane, Suite 400, Greenbelt, MD, 20770) and the OPSEC Professionals Society (OPS, 9200 Centerway Road, Gaithersburg, MD, 20879).

Let's Personalize the Process

There is nothing new about the principles underlying OPSEC. Although most employees do not consciously apply the OPSEC process in their personal life, nonetheless they do apply OPSEC. The next approach is to change their thought process, allowing them to clearly recognize how OPSEC is applied.

For example, if they have planned, or participated in giving, a surprise birthday party and took "steps" to ensure that the "mission" (keeping it from the birthday person) was successful, they practiced OPSEC.

Another example: When leaving for vacation, people understand the importance of having someone (a trusted insider?) pick up the mail, make sure the lawn is cut during their absence, stopping newspaper delivery, installing lights on timers, etc. Why? To prevent from being burglarized. But what have they just done? They are aware of a threat (a burglar), they don't want a burglar to know they are not home (the critical information), because there are vulnerabilities (or indicators) that can be compromised, and that the risk of a burglary exceeds the costs of…countermeasures. Sounds like OPSEC, doesn't it?

We are now making OPSEC more personal, with examples that employees can relate to.

But what about the "process?" The process, too, could take on a different approach (for OPSEC awareness purposes). For example, in order to enable a better understanding of the application of OPSEC let's reduce the number of steps from five to three (it's easier to remember three than five), yet maintain the intent of the process. And, rather than calling them "steps," let's call them "principles."

The First Principle of OPSEC:

*If you don't know the THREAT (adversary), how do you know WHAT to protect?**

Analyze the threat

The Second Principle of OPSEC:

If you don't know WHAT to protect, how do you know you ARE protecting it?

Identify the Critical Information

The Third Principle of OPSEC:

If you're NOT protecting it (the information) the adversary wins!

Analyze the Vulnerabilities
Assess the Risk
Apply Countermeasures

*Fortunately, NSDD298 was not mandating that each step be executed in the order in which they are listed. It may be necessary to identify the threat(s) first, then identify critical information requiring protection.

If there are no THREATS there would be no requirement for physical or personnel security – the "traditional" security programs. However, as security managers, planners, or OPSEC practitioners, we recognize that threats do exist, although specific threats can vary from site to site and from program to program.

The "WHAT" is the critical program information, or critical technology information (i.e., the target information) that adversaries require to meet their objectives. (Critical information need not be classified information.) Making up the critical information are the detectable activities and bits of data that can be pieced together (pieces of a puzzle) to derive the critical information (the puzzle picture).

Determining whether or not the critical information is being PROTECTED is a multi-phase process. The first phase involves conducting an OPSEC Assessment (OA) (some organizations refer to this as an "OPSEC survey"). An OA identifies, for example, what we do; how we do it; who we do it with; how we process, store, communicate, and dispose of information; etc., to identify if the detectable activities and bits of data are vulnerable to inadvertent compromise. In the event that information or indicators are vulnerable, then proposed "countermeasures" are evaluated to determine cost vs risk (consequence of loss). If, for example, the risk (consequence)-of-loss is far greater than the cost of a countermeasure, the decision-maker may decide to implement the countermeasure.

OPSEC and Personal Piracy...
Applying the OPSEC Principles

The previous section presented a different approach to understanding OPSEC in order to: simplify the OPSEC philosophy and process; and, to provide the OPSEC practitioner with an alternative methodology for instilling an OPSEC mind-set.

This section will underscore the necessity of personally applying the OPSEC principles. Failure to apply these principles could have serious, and long lasting, consequences. Each principle will be identified and demonstrated -- e.g., the threat will be presented; critical information will be identified; along with potential vulnerabilities, risk, and countermeasures.

The First Principle of OPSEC:

If you don't know the THREAT (adversary), how do you know WHAT to protect?

Analyze the threat

Y Threat

You've worked hard, saved, bought a home and car. Suddenly, and without warning, you are in jeopardy of losing it all. Why? Because **someone has pirated key pieces of your personal identifying information, and assumed your identity**. This "personal piracy" is called identity theft. If the resulting damage doesn't take you from "riches to rags," it could take you years to overcome.

According to Lt. Steven Franks of the Las Vegas (Nevada) Metropolitan Police Department's Fraud Squad, identity theft is "the crime of the future, occurring today, with the resources of yesterday."

In today's electronic age, we are more than ever susceptible to identity theft.

Lt. Franks also stated that "The impact of identity theft is significant. Nationwide, both the amount of loss and the number of reported cases are on the increase." Many criminals who commit crimes such as burglary, robbery, etc., are turning to identity theft. Why? Because, according to Lt. Franks who interviewed a robber-turned identity thief, "it is more profitable, there is less risk of getting caught, and, because it is considered a 'white collar crime,' the sentence could very likely be nothing more than probation."

The Second Principle of OPSEC:

If you don't know WHAT to protect, how do you know you ARE protecting it?

Identify the Critical Information

- **Identify the Critical Information**

Your identity can be stolen with just your **name** and **social security number**. In many instances your **date of birth** will be necessary. BUT.....other useful pieces of information that could be used to assume your identity may include your **bank account number**, **credit card number**, **signature sample,** and **driver's license number**. Even with your **car registration number** an identity thief could apply to the Department of Motor Vehicles, list a new address, and obtain a title to your vehicle.

The Third Principle of OPSEC:

If you're NOT protecting it (the information) the adversary wins!

Analyze the Vulnerabilities
Assess the Risk
Apply Countermeasures

- **Vulnerabilities**: Identifying Information-Collection Methods

Identifying vulnerabilities is the first phase of the third principle. Our OPSEC assessment (survey) has identified the following:

Y From Mail to Migraine

The Scene: A vehicle is slowly cruising the neighborhood. Suddenly the vehicle stops, the passenger gets out, goes up to a mailbox, and removes the contents. The indicator? A mailbox with the "flag" in the raised position. Back in their "safehouse," the mail receives scrutiny. Let's listen in…

Here's a pre-approved credit offer. Its got the bar code with the pre-approved information. All we need to do is change the address, send it in, and we've got it.

What luck. A W-2 (BIG trouble for you). *We'll just make up a phony tax return, with a sizable refund, of course. We'll change the address, file electronically, and have the refund before they know it. The IRS doesn't take kindly with filing taxes twice, but that won't be our problem.*

Look at this...a box of new checks, and the checks even have the driver's license number on them. We'll have their account drained by the time they realize that their checks haven't arrived.

A credit card statement. Now we know the credit limit...of course we could call the credit card company and ask for a higher credit limit...usually works.

What's this? Hmmmm...a wireless phone in their name just for sending in the card. We'll change the address. They probably think a lot of this stuff is just junk mail.

If the consequences of mail theft doesn't give you a headache…..

Y A "Change-of-Address" Can Be a Moving Experience

So, you haven't received mail for a few days? Unknown to you, an identity thief has submitted a change-of-address to the post office, listing a "drop box" as the new address. While this collection method may last only a few days before becoming suspicious, considerable damage could be done within that time, and you won't know what has been taken. And, there is less risk of the identity thief being detected.

Y And the Surrrveyyyy Says….

Be cautious about completing surveys. Many of the "surveys" ask for a considerable amount of personal information. You never know who, or how, the information will be used.

Y Treasures in the Trash

The scene: It is the early morning hours, there is no activity, except for a van that is driving slowly along the trash-can-lined street. The van stops, the passenger jumps out, grabs a trash bag and tosses it into the van. As they drive off one comments: *Dumpster-diving sure is easier when they use trash bags.* Back at their safehouse they dump the contents of the bag on the floor and begin sorting through "their find." Let's listen in…

Here's a Leave and Earnings Statement. Now we know who they work for. We have the social security number, date of birth, earnings... Hmmmmm, quite a lengthy employment and no sick leave credit...I wonder what that means?

Would you look at this...credit card receipts. This is great, now we know the credit card number and the expiration date. We even have their signature. I wonder if they realize that when ordering by phone that it is not an 'authorized transaction' until the expiration date is given. We'll start ordering merchandise by phone...

But we also know where this person eats, shops, goes for entertainment, travels....Boy...

Here's a bank statement, sure tells a lot, including the balance in their account... and guess what? Look at all of the ATM activity from a casino – and all are at the same place – good targeting information. You know, we could contact the bank, they probably use the mother's maiden name as the password...don't they realize that information is public record?

An empty packet of checks, but there are still deposit slips. We'll change the address, and send it to the bank requesting more checks. We'll start writing checks on Friday evening, and have their account drained, with overdrafts, by Monday.

Would you look at this! An expired credit card. I guess they knew enough to cut it in half, but we still have both halves. Even though it expired, we can figure out the new expiration date...same month but two years from now.

They just had their car serviced at the dealer. So, now we know the vehicle make, model, and identification number. We'll write to the Department of Motor Vehicles, give them this information, indicate that we lost the title, and get one.

Do you know what's missing from all of their discarded statements? No payments for alarm monitoring. I'll bet there is a lot of personal identity information what we could have access to.

The old adage "one man's trash is another man's treasure" sure works for us, doesn't it?

Y From Fax to Fiction

Sending a fax containing personal information? Unless it is sent via a

secure fax, it is subject to interception. Personal information may then be used for stealing your identity.

Y ATM - The Automated Theft Machine

The scene: You drive up to an ATM. Unknown to you there is a van in the parking lot where your actions are being video taped by the identity thieves. Let's listen in...

Wow, "shoulder surfing" sure is easier with this new camcorder...great zoom...and from here we can see the ATM keypad clearly. Too bad the last person took the receipt, it has the account number on it, plus it shows the account balance.

Let's see what this person does. Ouuuuuu, we got the PIN number. All right...the receipt is still in the machine, let's go get it.

Y From Card to Cache

Let's listen in as the identity thieves continue to discuss possibilities...

Know what I could do? I could get a job as a food server somewhere, think of the possibilities...most people pay for their meal by giving their credit card to the server, rather than taking it to the cashier. And they never look at the card when it is returned! I could substitute a stolen card that we've maxed-out for their card. Before they realize it...

But, better yet, see this little device that looks like a pager? It's called a "skimmer." I can swipe their card through it; it reads the mag-strip on the card and stores it...I then have the numbers...we can make our own card... Think of the possibilities!

Y From Purse To Pursued

The scene: Your purse or wallet is lost or stolen, and now in the possession of the identity thieves. As usual, we are going to listen in on their conversation...

Not much cash, but that's ok...look at all of the credit cards! You know, chances are that they will cancel the major ones, but forget the others. We can hit the stores before they know it.
And look, several gas cards....they'll work in the card reader at the gas pump. We'll gas up our van, and do the same for all of our friends.

We also have the driver's license. We'll just laminate my picture on top...cashiers never look that close, and since there are checks in this purse...

Look, a "debit card..." it's just like having more cash.

What's this? I think this is the PIN number!

I don't believe this!...here is the social security card...imagine...

Who do you think the merchants will be pursuing?

Y From Break-In to Bankrupt

The scene: You arrive home and find that the back door is standing open. Thinking that a burglary has occurred you assess the contents of your home to identify missing items. Everything is in order and it appears that nothing has been taken. You dismiss the open door, thinking that you must have forgotten to secure it when you left. However, let's listen to the identity thieves who were there earlier…

Looks like expensive stuff here. Gee, look at the jewelry...Someone else sure would find this to be a terrific haul. But we're not interested in that...what we leave with they won't miss. And they won't even know we were here, until it's too late.

Ok, the first thing we're going to look for is a computer....here it is. Let's see what we have...oops, password protected...hmmmm, what's this number taped to the bottom of the keyboard...let's try it. That's it...we're in. Now to check the programs. Hmmmm, a financial program...we'll just take a look. No password protection on this file. Wow, look at the balance in the checking account and savings accounts. We'll call the bank and transfer the savings to the checking. Guess what? There is a program for printing checks...this will be great for us.... Now for printing checks...we can print a number of them....but not with such a large amount that the bank will call them. We'll delete these entries when we're done. They will never know until they get their statement.

Yeah! Or calls from the bank that they don't have any money in savings OR checking. They probably think computer security is only for work!

Hey, let's see what's in the desk...A box of blank checks. We'll take the last pack...they'll never know.

Look what else is in the desk, neatly filed under "insurance." Their health insurance carrier and health plan number. I know someone who will buy this information. He'll get medical confirmation of his disability and apply to Social Security for disability payments, using this social security number. Doesn't he already collect disability benefits using other identities?

Ohhhhh. They have a brokerage account. We now have the Broker name, account number, stocks...lot's of great information here. We could call for a sale order and pick up the check at the office. This could wipe them out...Oh well!

*And a file of all of their credit cards, account numbers, credit limits...*wow!

Y Online? Bottom Line: You Could Become a Victim

The Internet is the "motherload" of information, providing the opportunity for easy, rapid, and cheap access to a wide range of

personal information that is just a few keystrokes away. What have you already given away?

Many web sites place files called "cookies" or "Web Bugs" to track a computer user's movements through cyberspace, including purchases. Some programs have the capability to collect personal information, research data on your hard drive, or cause damage to your system. Running in the background on the web browser, this collection is transparent to the user. (For more information: www.grc.com.)

Y From Badge to Bad News

The scene: It is a Friday afternoon, you park in the lot of a social club. You use the remote to alarm your vehicle and head for "happy hour." Let's listen in to the identity thieves, who are parked nearby…

This is terrific...we're about 60 feet away, and yet this little device still picked up the alarm-remote code. For twenty bucks, this device sure has come in handy. Now we'll reprogram our remote and disarm that car. Let's see what's inside.

A badge hanging from the rear-view mirror. Hey...isn't that the company that does all that secret work? I've seen it...it's completely fenced, but they have these big turnstile gates, no guards. Since it's Friday, the badge won't be missed until Monday; people just get a temporary badge anyway, thinking they'll find it. So, we'll get inside and see what we can see. I wonder if we could sell this badge to their competitor?

Here's a check book. We'll take some of the checks from the back -- they won't be missed...until it's to late. I'll laminate my picture on the badge...a bank teller probably won't know the difference. I'll cash these checks at different branches using the badge as ID. The account will be drained.

Boy...bad news when the security office and bank find out!

Y From Phone to Moan

Our identity thieves are at work obtaining personal information in order to assume another identity. Want to know what they're up to?

We need some more information on this person. I'll call them, identify myself as an 'Account Verification Representative' and that I am verifying their account information, including current password. If I say the right 'buzz words,' and sound official, I'll bet they fall for it and give me what we want to know...this usually works.

Yeah, it's surprising what people tell us over the phone. Imagine their reaction when they figure out what they've done...Ohhhhhh Nooooo!

Y E-mail: Detail

The identity thieves are still at work…

Oh my gosh! Come and look at this e-mail...all this detail...including a meeting that they will be attending..it shows when they're leaving, the airline, where they're going, their hotel, how long they will be gone, even the meetings they will be attending! This sure gives us a better idea of what they do.

Don't they know that e-mail is not a secure way to communicate?

And look at the distribution list...wow!...must be all of the top people in this "program!" Imagine the damage we could do by also taking the identity of ***these*** *people also.*

Y From Lease to Fleece

The identity thieves are kicking back at their safehouse. Before we leave them, let's listen in one more time:

This sure has been a nice house, I'm going to miss it. But we've lived here for several months and not paid any rent...we're about to be evicted.

Yeah...but since we leased this house under a stolen identity, they won't be looking for us. I guess I should be looking for another house to lease...under another name, of course.

These are just some examples of information vulnerabilities. Now that you have the concept, what additional information vulnerabilities can YOU develop?

Y **Assessing the Risks** (consequences)

Assessing the risk(s) is the second phase of the third principle.

If your identity is stolen it can be corrected, but it could take years, involve numerous hours on the telephone, untold letter writing, preparing and submitting affidavits, etc. In the mean time you may not be able to purchase a home, car, obtain credit cards, or open a checking account.

You could also be arrested for criminal activity committed by an identity thief who used your name, date of birth, and social security number when arrested.

You're involved in a traffic accident; the police arrive and arrest YOU for -- unknown to you -- outstanding traffic violations; your driver's license has been suspended

because of the outstanding violations; your car registration has been cancelled, as has your insurance. Why? Someone stole your identity.

Or, the Internal Revenue Service could be looking for you for unreported income on your tax return -- because someone was working with your identity -- or for filing more than one tax return, because someone else already has.

Y Apply Countermeasures

In situations where there is a threat, critical information is vulnerable to compromise, and there are risks (consequences) involved, then countermeasures need to be evaluated in relation to the risk. In this phase of the third principle, we will compare the cost of several proposed countermeasures with the con sequence (risk) involved.

Y Protect incoming and outgoing mail from theft. Deposit outgoing mail into a post office collection container. If your mailbox is not secure, consider a post office box.

Cost vs Consequence: _____

Y Better shred than read. Shred all documents, credit card receipts, statements, etc., even though you may consider some items as "junk mail."

What kind of shredder? A "strip" shredder may not be good enough. Lt. Franks commented that an identity thief was apprehended and when his residence was searched, they found "strip shredded" documents that had been taped back together. Better: a cross-cut shredder, for a few dollars more.

Cost vs Consequence: _____

Y Purse or wallet. Do not carry your social security card. Limit the number of credit cards that you carry to the absolute minimum. Do not carry your PIN or password.

Cost vs Consequence: _____

Y Statements. Be aware of when credit card, bank, and other statements are due. Follow up if statements have not arrived on time.

Check all credit card, bank, and other statements carefully for any unauthorized entries.

Cost vs Consequence: _____

Y PINs & Passwords. Do not use obvious PIN or passwords, such as your date of birth, last four of your social security number, mother's maiden name, etc. Make up a password or PIN that someone else could not easily determine, such as your favorite food, or a phrase (e.g., "my dog is spot" – the telephone pad number corresponds to the first letter of each word - 6347).

Cost vs Consequence: _____

Y Telephone, internet, and other communication precautions. Do not give out personal information unless you have initiated the contact or know, <u>for sure</u>, who you are dealing with (banks, credit card companies, etc., with whom you do business, already have such information). And remember, conversations over the cordless or cell-phone can be intercepted.

Cost vs Consequence: _____

Y Social Security Number. Provide your SSN only when ABSOLUTELY NECESSARY.

Cost vs Consequence: _____

Y Protection Measures at Home:

Computer. Do you have personal and other sensitive information stored on your computer? Use password-protection and, as an added precaution, password-protect various sensitive files. (Don't post your password(s) under the keyboard, behind the monitor, etc.)

Maintaining and Storing Sensitive Information. Keep a record of all credit card numbers as well as phone numbers to report lost or stolen cards. BUT…keep such information in a secure place (consider a fire-resistant combination repository, secured with "security screws" in an inconspicuous location).

Cost vs Consequence: _____

Y Car Concern

Even with a car alarm, the contents of your car are vulnerable. Do not leave identifying documents inside (including car registration and insurance documents). The trunk, although not totally secure if there is a "trunk release," is still better.

Cost vs Consequence: _____

These are some examples of the possible measures that could be implemented in order to protect vulnerable information. Now that you have the concept, what additional measures would YOU recommend?

Identity theft. You are the Program Manager (decision maker). Considering the consequences of losing your information, and comparing the cost of implementing the suggested measures, **what would be your decision** -- would you accept the risk? Or, would you apply one or more of the countermeasures?

IN CLOSING.....

The examples presented in this article are clear, and practical, applications of the OPSEC process. Using a real-life scenario, we have identified a threat, and information that requires protection; then developed several measures to protect the vulnerable information, along with the cost/consequence. This was done with a program called..."OPSEC."

Jeopardy is not just a game show. Don't place your job, career, and everything you've worked and saved for, in jeopardy. Practice OPSEC, whether at home or at work. The risks are too great to treat OPSEC casually -- Take It Personally.

OPSEC: Convinced? Or Confused?
Want to know more? www.nv.doe.gov/opsec