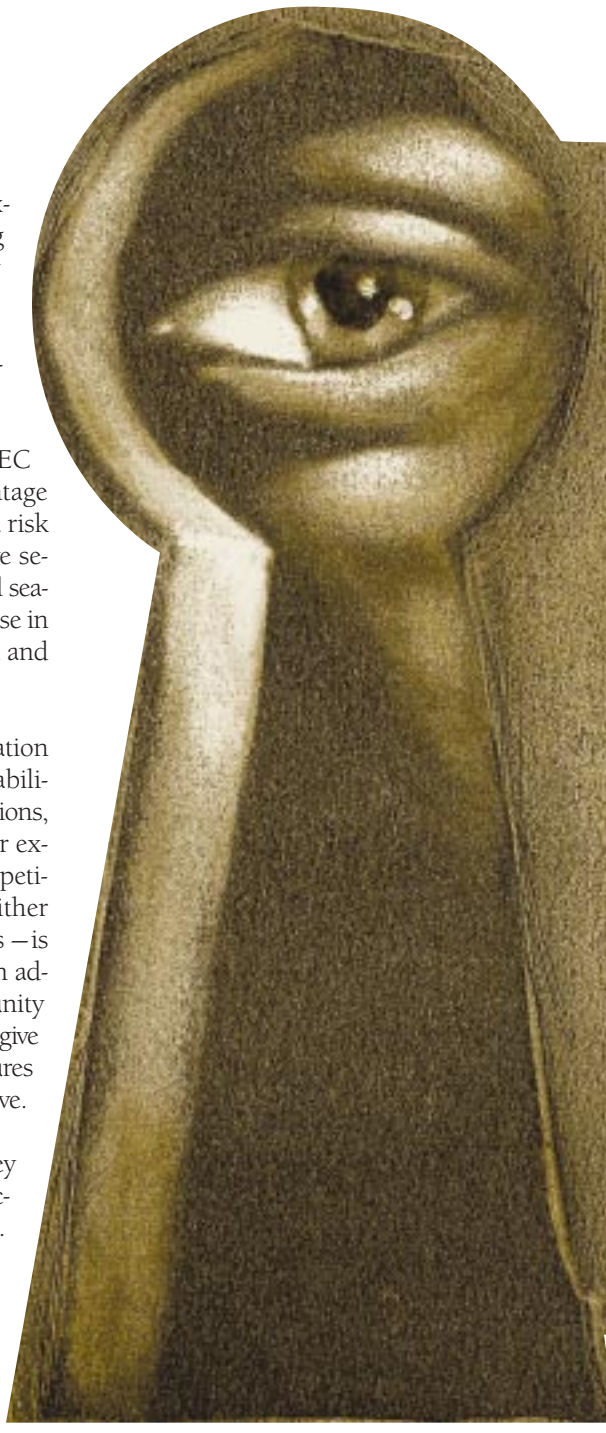
The Operations Security Connection

Security Risk Avoidance *Out* – Security Risk Management *In*

ARION N. "PAT" PATTAKOS



"Some elements of the intelligence and defense community have been using the risk management process for many years under the rubric of Operations Security (OPSEC)," notes the Department of Defense/Director of Central Intelligence, Joint Security Commission Report, *Redefining Security,* issued February 28, 1994.

A Paradigm for All Seasons

If you follow U.S. government security issues, clearly DoD's prevailing paradigm actively promotes security risk management techniques to achieve a sensible security posture. In brief, security risk avoidance is *out* (too expensive), and security risk management is *in* (a rational consideration of cost and benefit).

Definitions of risk management abound. One such general definition simply states that it is a method of managing that concentrates on identifying and controlling the areas or events that have a potential of causing unwanted change...it is no more and no less than informed management. Unwanted disclosure of critical information falls well within this definition, due to its high propensity for provoking "unwanted change."

The security community's proposed "new" security risk management paradigm, as advanced at the national level by the Security Policy Board, is promoted for government-wide use. If you examine the 30+ years of using OPSEC's proven process, it readily becomes apparent that it makes sense in all organizational environments where adversaries or competitors can cause you pain.

Once you understand the OPSEC process, you have a distinct advantage in understanding and promoting a risk management approach for effective security. It literally is a paradigm for all seasons – adaptable and flexible for use in determining what assets to protect and how to protect them.

OPSEC's goal is to control information concerning your operational capabilities, limitations, activities, and intentions, thus preventing or controlling their exploitation by an adversary or competitor. Operational effectiveness – either government or business operations – is inevitably enhanced by denying an adversary or competitor the opportunity to foresee your intentions, and thus, give them the opportunity to take measures to nullify any advantage you may have.

If you apply OPSEC measures, they will maximize your potential for success in any competitive environment. In essence, OPSEC seeks to prevent adversaries/competitors from gaining your critical operational information.

Pattakos is Director of Programs Integration for Beta Analytics International, Inc., and has served in the public and private sectors. A retired Army colonel, his military career included staff positions as Secretary to the Joint Chiefs of Staff, and Deputy Chief of Staff for Operations, U.S. Intelligence and Security Command; as well as command positions with the Army's Intelligence and Threat Analysis Center, the Operational Group, and the 902d Military Intelligence Group. In his present position with BAI (a full-service security firm), he ensures that program managers have the information resources they need to support government and commercial clients. He is an OPSEC Certified Professional (OCP) and a Certified Protection Professional (CPP).

Operational effectiveness — either government or business operations — is inevitably enhanced by denying an adversary or competitor the opportunity to foresee your intentions, and thus, give them the opportunity to take measures to nullify any advantage you may have.

OPSEC Analytical Process

The OPSEC analytical process focuses on the adversarial exploitation of open or public sources and observable actions to obtain evidence of critical information. These sources are generally Unclassified (not protected as "proprietary information") or are observable activities with no classification. (Proprietary information is the business equivalent of the government system of protecting and safeguarding classified information.) Consequently, such sources of information may be more difficult to control than those that are classified or protected as proprietary.

Since traditional security programs generally protect classified or proprietary information, OPSEC's process focuses on identifying those indicators that contribute to the loss of critical information. It does so by pinpointing those indicators that are not protected, and taking action to deny or control their availability to an adversary or competitor.

Further, OPSEC measures complement other security measures — physical, information, signals, computer, communications, and electronic — to ensure a totally integrated security package. In fact, stepping through the OPSEC process will likely disclose weaknesses in the application of traditional security practices.

How? OPSEC looks at your behavior from an adversary's or competitor's point of view. Information that they need to achieve their goals to your detriment constitutes what you want to protect — the critical information of your operations or activities. To deny this critical information to adversaries/competitors contributes to your own operational effectiveness.

The OPSEC Process

Normally, OPSEC deals with information that, collected in pieces and combined in aggregate form, could reveal sensitive or classified (business proprietary) aspects of an operation or activity. Thus, OPSEC uses a systematic process, designed to determine how adversaries and competitors derive critical information in time for them to exploit that information and use it to your detriment.

The five steps of the OPSEC process are not observed in a rigid sequential order. A recognized strength of this process is its flexibility, thus enabling the OPSEC practitioner to shift back and forth from one step to another, in any order, and any number of times. This flexibility facilitates the effort of achieving operational effectiveness by denying critical information to an adversary.

Practitioners depict OPSEC in different ways. Some depict the steps in the form of a cycle because of their changing, dynamic nature. Another depiction (as shown on p. 38) is three partially overlapping circles denoting critical information, threat, and vulnerabilities. Where all three circles overlap, you have risk and a potential need for countermeasures to mitigate that risk.

As the various elements impacting on your security decrease or increase (for example, the value of information, the seriousness of the threat, and the vulnerabilities a threat might exploit), so must risk decisions change. This Venn Diagram representation is popular with the growing security risk management community.

A discussion of OPSEC's five steps follows:

Identification of Critical Information

This is the information required by an adversary to achieve their goals. A more formal definition of critical information is *specific facts about intentions, capabilities, and activities vitally needed by adversaries or competitors for them to plan and act effectively so as to guarantee failure or unacceptable consequences for your mission accomplishment.*

If you rename this step *Critical Asset(s)*, the five steps of the process can be used in any situation requiring an analytical security risk management approach. Such critical assets might be people, information, equipment, facilities,

activities, or operations. A point to remember is that protecting any asset — from a building to a person — involves some information component, and the protection of this information may be critical to protecting the asset.

In this step, you determine the adverse impact that an undesirable event might have on your asset. In terms of a weapons system, for example, consider this question: May an adversary's exploitation of your information on a weapons system lead to that system's being countered, killed, cloned, or force you into a major redesign?

Analysis of Threats
In this step, adversaries and competitors are identified, including their goals, capabilities, and intentions.

- What do they know?
- When did they know it?
- What do they want?
- Why do they want it?
- How do they go about getting it?

Analysis of Vulnerabilities
This step involves an examination of your total operation or activity, including scrutiny of any vulnerabilities for indicators of critical information that may be exploited by a threat. An adversarial approach is used; that is, we put ourselves in the position of an adversary and study our operations and activities step-by-step, in all phases, from an adversary or competitor's perspective.

Adversary attack scenarios are developed to disclose paths they might use to gather our critical information. We then determine any correlation between our operational actions and an adversary's exploitation capability. Another consideration is how long information may be of value compared to an adversary's ability to collect and exploit the information within that time frame.

Assessment of Risk
In this step, the risk analyst integrates the preceding steps (critical information, threats, vulnerabilities). This is the decision step of the process — at this point decision-makers receive the analysis, together with recommended countermeasures designed to mitigate the risk.

One outcome of this assessment is a prioritization of risks. Countermeasure costs (in dollar terms, operational impact, etc.) are related to the value of the asset, while benefit is related to the amount of risk reduction the countermeasure offers.

Applications of Appropriate Countermeasures
Countermeasures are actions that deny or reduce the availability of critical information to an adversary or competitor. OPSEC countermeasures may be categorized as: 1) elimination of indicators subject to exploitation; 2) disruption of effective adversary collection or processing efforts; or, 3) prevention of the accurate interpretation of indicators during an adversary's analysis. Thus, the principal impact of a countermeasure is to reduce one or more vulnerabilities.

It should be recognized that the application of some countermeasures might cause another vulnerability. For example, posting guards to protect an activity might focus undesired attention on that activity. Thus, as part of the OPSEC cycle, prudence requires that you evaluate the effectiveness of your countermeasures the same way you monitor any changes in the value of your assets, the threats to those assets, and the vulnerabilities a threat might exploit.

In the Final Analysis

Security risk management is *everyone's* job. By using the OPSEC analytical process, government executives or business decision makers and managers — *you* — will have a better understanding of what information may be available to an adversary or competitor, the impact of losing that information, and a better understanding of ways to protect valued assets and information. In so doing, you are also selectively applying the "new" security risk management paradigm and, ultimately, contributing to overall organizational effectiveness.

Editor's Note: The 10th Annual National OPSEC Conference and Exhibition will be held March 21-24, 1999, at the Radisson Hotel at Mark Center, Alexandria, Va. Those interested in attending should call (301) 840-6770.

The OPSEC Process