

Using Operations Security Techniques to Reduce Security Risks and Security Costs

by George F. Jelen

In most companies, although the need for security is recognized and appreciated, its rising costs and the increased drive to reduce expenditures have made it a frequent target for budget cuts. The success and even the future survival of security departments may depend on their ability to manage and contain department costs effectively.¹

As resources for security grow more scarce, it becomes ever more important that available security resources are applied where they can do the most good, and that any reductions be made intelligently. It is necessary to distinguish between what really needs protection and what does not. Some mechanism is required that allows the prioritization of security needs according to some rational process. An ideal process would at once be rational, convincing, repeatable, and reasonably simple.²

Such a process should weigh the importance of the information, the motivation and the capabilities of our competitor, the ease with which that competitor could obtain that information, and the risk of leaving a given secret unprotected versus the cost of protecting it. This is exactly what the methodology of Operations Security offers. The process associated with Operations Security imposes a rigor that can be profitably employed in many security resource decisions.

Operations Security, or OPSEC, was initially developed during the Vietnam War in response to evidence that the North Vietnamese had advance knowledge of U.S. air operations. It involves a systematic analysis of an organization's own activities looking for ways by which adversaries might discover information critical to the organization's success, and then taking action to reduce or control this information so as to prevent or limit its exploitation by such adversaries. This "critical information" can take the form either of publicly available information or actions observable to the adversary. OPSEC involves the application of a systematic analytical process to determine how adversaries derive critical information in time to be of value to them.

OPSEC and Security Risk Management

Security resources are applied in order to reduce security risk. Since security resources are not unlimited, their effective management is equivalent to the effective management of security risk. Available security resources need to be applied in such a way as to minimize this security risk.

The discipline of OPSEC offers a proven approach to security risk management. A recent study of the U.S. government's security policies and procedures specifically advocated a risk management approach that closely resembles the OPSEC process.³ This study, conducted by a commission appointed by the Secretary of Defense and the Director of Central Intelligence, was composed of ten distinguished Americans and known as the Joint Security Commission.

As defined by the Joint Security Commission (JSC), Security Risk Management applies a five-step process. Operations Security also employs a five-step process. While the five-step process described in the JSC report is not identical to the process described in the "National OPSEC Doctrine,"⁴ the two processes are equivalent. The largest difference between them is that the JSC report divides the Risk Assessment step of the familiar OPSEC process into two steps and only implies the fifth step, "Implementing Countermeasures," rather than stating it explicitly as a discreet step.

The five-step process, as defined by the JSC, consists of:

1. asset valuation and judgment about consequences of loss—determining what is to be protected and appraising its value;
2. identification and characterization of the threats to specific assets;
3. identification and characterization of the vulnerabilities to specific assets;
4. identification of countermeasures, costs, and tradeoffs; and
5. risk assessment.⁵

The OPSEC Process

The five steps of the traditional OPSEC process are quite similar, consisting of

1. the identification of critical information—that information the adversary needs to achieve his or her goals;
2. analysis of threat-identifying adversaries, their goals, intentions and capabilities;
3. vulnerability analysis—an examination of the total activity for indicators of critical information that can be exploited by a competitor;
4. risk assessment—an estimate of the potential effects of a vulnerability on an operation and a cost-benefit analysis of possible corrective actions; and
5. application of appropriate countermeasures—cost effective actions which deny or reduce the availability of critical information to a competitor.

Each of these steps or phases is important to the integrity and efficacy of the overall process. Although each of them has value in and of itself, it is only when all five are employed together that the full synergistic value of the OPSEC process accrues.

Identification of critical information provides focus. If you do not take the time and make the effort to identify the particular information that the adversary needs to achieve his or her goals, with the intent to focus your protection resources on such information, you will easily find yourself trying to protect all information equally. This makes no sense and you probably could not afford to do it even if it did.

Threat analysis assures realism. Just as it is not possible to protect all information, it is also not possible to protect any information against all threats. To be worth protecting against, a threat has to be realistic. Competent threat analysis assures this.

Vulnerability analysis lends objectivity. The critical element of a vulnerability analysis is placing ourselves in the position of the adversary as we examine our own processes. We attempt to view our own operation through the eyes of our opponent. Forcing ourselves to look at ourselves as others see us is what brings objectivity to the overall effort.

Risk assessment guarantees rationality. Fundamental to the OPSEC discipline is the tenet that not all vulnerabilities are worth correcting. Deciding which ones are and which ones are not is the task of the risk assessment step. Thus the risk assessment phase is key in ensuring that the overall process succeeds as a means of managing risk. Absent a fairly rigorous assessment of the risk, the practice of OPSEC quickly degenerates into little more than a search for matches between threats and vulnerabilities. Unless such a search is followed by a prioritization of threats and vulnerabilities and some kind of cost vs. benefit analysis, the application of countermeasures becomes an exercise in risk avoidance. The rationale necessary for intelligent countermeasure decisions is missing.

The application of countermeasures ensures utility and value. If one fails to follow through to the application of appropriate countermeasures, the entire effort amounts to nothing more than an intellectual exercise and accomplishes nothing.

Taken together, these five steps do indeed represent a logical and balanced approach to contending with risk. The point, however, is that one has to complete all five of them. Because the critical information step is what lends focus, if that step is omitted, the analysis is unfocused. Similarly, if the threat analysis step is dropped, the process lacks realism. Absent an adversarial analysis of vulnerabilities, it would not be objective. If we skip the risk assessment (which seems to be the most frequently omitted step), the effort lacks rationality. And, if we fail to follow through to the application of countermeasures, it has no value. The real power of the OPSEC process results from the combined contribution of all five steps. Leaving any one of them out robs the process of that power. The report of the Joint Security Commission made the same point. Commenting on their own five-step risk management process, their report notes; "When any of the steps are left out, the result can either be inadequate protection or unnecessary and overly expensive protection."⁶

I am not saying that, if you omit a step, the effort is without any value at all. Every one of the steps has value by itself and any combination of them has that much more. But I am saying that, if you omit a step, not only do you deny yourself the full benefit of the process, but by definition, what you end up practicing is not OPSEC. OPSEC is defined by its process.

A basic premise of the OPSEC discipline is that not all information merits protection. Currently, far too much money is spent trying to protect information that is either not worth protecting, is already known, or is fundamentally unprotectable. This makes no sense and no organization, business or government, can afford to continue to do it. The application of the Operations Security discipline and its methodology can be extremely useful in helping an organization sort out what most needs protection and in making sensible decisions about where—and where not—it can best afford to cut resources.

A New Paradigm

For most security people, this OPSEC or risk management process requires a whole new way of thinking and of approaching the problem—in other words, a paradigm shift. The old paradigm looks at the problem from the inside out; the new paradigm looks at the problem from the outside in. Suppose you have some project or activity you wish to protect, and you decide to get some outside professional advise. So you call in a couple of professionals; you call in a traditional security expert and you call in an OPSEC professional. As you describe your problem to them, both of them are going to ask you some questions. The first question they will probably both want you to answer is just exactly what is it you wish to protect. But the second question will be different. The second question the traditional security professional is likely to ask is *how can whatever it is be protected*. The second question the OPSECer is likely to ask is *how could the adversary get it*. Very different questions! Both are good and valid questions. Both deserve to be asked and both deserve to be answered, but they lead in different directions. The traditional security approach looks at the problem from the inside out. It attempts to create some barrier around whatever it is that needs protection. The OPSEC approach, on the other hand, is an outside-in approach. It looks at the problem from the point of view of the adversary or competitor who wants whatever it is that one is trying to protect. Because the two approaches are different, they complement each other.

Whereas the old paradigm has tended to focus on system strengths, under the new paradigm the focus is on weakness. This is a natural consequence of assuming the perspective of the competitor. The competitor is not looking for those aspects of your security system that are the strongest; he is looking for those aspects that are weakest—those that he can most easily exploit. Whereas persons operating under the old paradigm tended to define critical information as that information of most value to themselves, those operating under the new paradigm define critical

information as that of most value to their competitor. Under the old paradigm we generally protect only what is legally required, while under the new paradigm we protect indicators of critical information. Under the old paradigm one would only concern oneself with what a document might contain;

under the new paradigm, one would also need to consider inferences derivable from what the document did not contain. And whereas the old paradigm attempted to enforce a set of rules and regulations, the new paradigm leaves much room for judgment and therefore attempts to instruct people how to discern and make thoughtful choices.

The Unique Contribution of OPSEC

Equally important to avoiding the protection of information that does not warrant protection is assuring the protection of that which does. Having identified the information most in need of protection, it is no less critical that such information be protected consistently and completely—that money is not spent on a robust lock for the front door while the back door is left unbolted. A mechanism is needed for injecting some discipline into the process—for assuring that once a decision is made to protect a particular critical piece of information, it is protected uniformly and consistently throughout the organization. Here again, OPSEC can be helpful.

I pointed out earlier that the processes of OPSEC and Security Risk Management are equivalent. However, their focus is somewhat different. The primary focus of OPSEC is on protecting against indirect loss of critical information. It generally leaves to other security disciplines the protection against direct loss and it does not greatly concern itself with losses that cannot be related to information losses. Security Risk Management is a more general concept whose focus would not be limited to protecting information and would even include protecting against natural disasters or sabotage, for example.

I recall a situation that occurred a couple of years ago. An experienced OPSEC professional was asked to address a small class of intelligence professionals on the subject of Operations Security. As a way of introducing his subject, he asked the group this question; "All of you are intelligence professionals. I'd like to know how much of the intelligence product that you produce is based on direct sources—a captured document or manual, a photograph, a HUMINT source, a SIGINT intercept—and how much, on the other hand, is the result of careful analysis, assembling many little pieces of information to form a complete picture?" The class discussed this question briefly among themselves before coming up with a collective answer "Ten and ninety," they replied. "Ten percent is based on direct information and ninety percent is the result of analysis and inference." "Well," said the OPSEC professional, "I'm in the business of protecting the ninety percent."

There are two points to this story. The first is that the 10/90 split was not what the intelligence professionals would have preferred. The reason that only ten percent came from direct sources was because the traditional security disciplines were doing their job in limiting access to those sources. The second point, however, is that in spite of the effectiveness of the traditional security disciplines, the intelligence analysts were not put out of work there was still plenty of intelligence to produce. The analysts simply had to work harder to get it. By specifically addressing the indirect sources, the ninety percent, the discipline of OPSEC seeks to make that analysis work harder still.

The various traditional security disciplines generally do an excellent job of protecting against direct disclosure. But secrets can be revealed indirectly as well as directly, and OPSEC complements these other disciplines by seeking also to protect those same secrets against indirect disclosure. Failure to consider ways in which a competitor might piece together the same secret from bits and pieces of information could mean that a considerable amount of money is spent in security protection but the secret is given away anyway. Without Operations Security, the envelope of protection is likely to be incomplete.

Ultimately, OPSEC protects against inference. It seeks to limit the competitor's ability to infer. Inference has been defined as "a statement about the unknown made on the basis of the known."⁷ It has innumerable sources, some of which can be very obscure. Inferences can be made from stereotypical patterns or deviations from such patterns—from some particular activity or from the absence of such activity.

I recall a conversation I once had with a Secret Service agent. The agent had formerly served as a member of the presidential protection detail and was explaining to me how their advance teams work. He related how these teams would be sent to a distant city a few days before the scheduled arrival of the president. He stated that the advance team always carried with it a checklist and that this checklist, although not formally classified, was considered quite sensitive. By way of explanation, he pointed out that the Secret Service agents would not want any would-be assassins to get hold of the list, to see what was on it, and therefore to know what the agents were checking. I told him that I understood that the checklist was sensitive but that he had explained it wrong. Looking slightly offended at my bluntness, he asked what I meant. I said that if I were the would-be assassin, it is not what is on the list that would interest me. What I would want to know is what was not on the list; I would want to know what the agents were not checking. He looked at me rather strangely and said,

"Gee, that's right. I never thought of that." He had been viewing the situation from his own point of view. Years of prior experience in intelligence allowed me to see it more readily from the point of view of the would-be assassin.

However, the story does not end there. In spite of the fact that I was able to make this specific observation immediately, it was a full year later before I came to a full understanding of what I had observed. What finally occurred to me, as I was relating this story, was that frequently it is not what is present that is most significant or revealing; rather it may be what is missing. Important inferences can be drawn both from what is present and what is absent.

A similar situation has sometimes arisen during the questioning of persons arrested and charged with espionage. Such persons, when apprehended, are interrogated with the objective of assessing damage, to such circumstances, the interrogators are very interested in the questions asked by the accused's former handlers and by what he told them. But occasionally, the questions not asked are even more revealing. When significant information to which the accused had access generated no interest on the part of his handlers, the interrogators might reasonably conclude that there is still another spy who has not yet been caught. Because the goal of OPSEC is to protect against inference and because inferences can be drawn even from events that do not take place, OPSEC can be extremely subtle.⁸ OPSEC, to be effective, must consider and deal with all possible sources of inference.

The New Threat

While recent world events may have changed the threat to the government's national security interests, the threat to commercial interests may be greater. For the last half century, countries devoted their most advanced technology and most skilled people to the conduct of espionage against targets of governmental interest. This is no longer the case. As one writer recently put it

Today the victims, sponsors, and practitioners of the post-World War II espionage revolution are found in the international economic marketplace in the guise of supply and demand, most specifically in the United States with its leading technical and economic position as well as its time-honored philosophy of free enterprise and business opportunity.⁹

What was once viewed as a murky business has become a dignified profession—a legal and ethical enterprise.

To maintain a competitive position, many firms are now creating intelligence organizations and strategies to obtain competitive business data.¹⁰ Reported cases abound, ranging from rummaging through a competitor's trash to bribing one of its employees. And although the more dramatic cases get the headlines, the bulk of the work is far more pedestrian. As one report points out, "the lion's share of the work is building pictures from disparate bits of information by inference and extrapolation."¹¹ The object of such efforts is the proprietary business information of a firm's competitor. Given this fact, it becomes prudent for firms to protect themselves from such collection. OPSEC provides a means of doing so. OPSEC can be used to shield sensitive business information from competitors by first identifying and then taking steps to limit and control public data and externally visible activities that might reveal sensitive business plans or activities.

OPSEC is especially geared to such competitive situations. In a competitive situation, an adversary's success comes at the expense of our own. Our cause is advanced whenever that of our competitor is foiled. And since our adversary's strategy involves trying to thwart our success, we increase our effectiveness whenever we call frustrate that strategy, if your competitor's strategy includes an organized intelligence collection effort directed against your company, OPSEC measures are particularly useful.

Vulnerabilities

Typically, in a given situation, there are many ways in which important business information might be revealed to a competitor. These various ways can be viewed as system or process vulnerabilities. Not all of these vulnerabilities are worth correcting. A weakness or vulnerability hampering the protection afforded to a particular element of information is worth correcting or reducing only if there is some competitor who wants the information. Because the objectives of different competitors vary, what must be protected from one is likely to be quite different from what must be protected from another. And, if all of the various ways in which a particular piece of critical information might be revealed to a competitor are ranked as to their ease or likelihood, it makes little sense to spend much money to correct the fifth vulnerability on the list if there is nothing that can be done about the second. In addition, sometimes the elimination of one vulnerability introduces another. Occasionally, for example, the imposition of some physical security barrier only succeeds in calling unwanted attention to the most sensitive aspects of an operation. Because a cost/benefit analysis of proposed countermeasures is part of the OPSEC process, the application of that process guarantees that the gain vs. the loss resulting from the elimination of each vulnerability is independently assessed.

There are many sources of OPSEC vulnerability. But what we have discovered ever the years is that most of them are in the support areas. More often than not, what we call OPSEC indicators occur in activities involving the movement of people, money or things—in other words, in support functions like personnel, travel, finance, and logistics. From an analysis of actions and data associated with these activities, one can deduce ways in which adversaries might obtain an organization's critical information, even when effective security measures to deny access to all relevant classified and sensitive information are in place.¹² This analysis of actions and data, as well as the protection from indirect revelation, is basic to the practice of Operations Security.

To succeed in OPSEC, one has to think of everything—in advance. It is exactly what one forgets or fails to consider that can lead to an OPSEC failure or breakdown. Even when planning something as mundane as a surprise birthday party, it is very difficult to anticipate and deal with ahead of time all of the myriad ways the secret might be revealed—particularly if the person for whom the party is being planned is a spouse or roommate. Suppose, for example, that when placing the cake order with the bakery, the party planner neglects to caution the bakery that, in the event of any question with the order, not to call him or her at home. For, should such a clarification be necessary and the bakery makes the call, there is a very reasonable chance that the spouse or roommate might answer the phone, and once the bakery identifies itself and the reason for the call, the secret is blown and all of one's careful planning and execution goes for naught.

During the last four or five years, more and more organizations have come to recognize the value of the OPSEC methodology. As a result, the OPSEC process is now seeing application in a rapidly widening set of circumstances and activities. Since its initial application to military operations during the Vietnam War, the Secret Service has applied it to personnel protection, the FBI to law enforcement, the defense community to weapon system acquisition, the Coast Guard and the Customs Service to drug interdiction, and the Intelligence Community to sensitive operations. Although there is very limited experience in applying OPSEC in fields or situations other than these, it should prove relevant and useful in any situation involving at least two participants, each seeking some advantage over the other, as in any form of competition.

Summary

In summary, OPSEC's purpose is to enhance operational effectiveness; it employs the methodology of intelligence analysis; its point of view is that of an adversary or competitor; its focus is on information critical to that adversary and to his or her purpose; and it is unique in that it does not exclude any useful sources of information, even indirect and inadvertent ones. OPSEC specifically protects against inference and is applicable in any competitive situation.

The value of Operations Security lies in its ability to complement other security disciplines by augmenting and completing the security protection provided by them. It offers an effective means of managing risk and can be useful in security resource decisions by providing both a context for those decisions as well as a reasonable means by which such decisions can be made. Not only can it help avoid expenditures that are not necessary but it helps to provide documented justification for those that are. If applied or implemented properly, it should yield a cost savings, either by avoiding unnecessary or ineffective expenditures for security, or by averting larger downstream costs that would result from an adversary or competitor deriving advanced information regarding your intentions or plans. OPSEC will allow your security assets to be directed where they will do the most good, and you are likely to discover that you can eliminate some as well.

Applying OPSEC to security resource decisions can sometimes yield dramatic results. For example, when the U.S. was preparing for the arrival of Soviet inspectors as a result of the Strategic Arms Reduction Treaty, teams went around to a number of contractor facilities and Air Force bases looking at what special security arrangements would be required. Applying the OPSEC methodology, the teams were able to reduce the projected expenditures for security by several tens of millions of dollars. In fact, what many in the OPSEC profession have come to realize is that if OPSEC isn't saving you money, you haven't gotten it right yet. This is more than a slogan. As indicated above, there are real situations in which the application of the OPSEC methodology has yielded significant cost savings. It could do the same for you and your company.

Because it is subtle and abstract, OPSEC is hard to explain and is often misunderstood. Although usually straightforward and logical, it is nevertheless very difficult to master. But since it can yield important and tangible benefits, particularly in today's world of uncertain threat and reduced security resources, mastering OPSEC is worth the effort it takes. Even if a company is not ready to implement an OPSEC program inside the organization, it may be wise to consider applying its process to help it contain costs and otherwise manage your shrinking security resources.

NOTES:

1. Ann C. Northcutt, "Master the Budget, Line by Line," *Security Management*, Vol. 35, No. 7 (July 1991), p.54.
2. George F. Jelen, "OPSEC for the Private Sector," *Security Management*, Vol 38, No 10 (October 1994), p. 67.
3. U.S., Joint Security Commission, *Redefining Security: A Report to the Secretary of Defence and the Director of Central Intelligence*, 22 February 1994, pp. 5-6.
4. U.S., National Operations Security Advisory Committee, *National Operations Security Doctrine*, dated January 1993, distributed by The Interagency OPSEC Support Staff.
5. Joint Security Commission, *Redefining Security*, p. 5.
6. Joint Security Commission, *Redefining Security*, p. 6.
7. S. I. Hayakawa, *Language in Thought and Action*, Fourth Edition (New York and others Harcourt Brace Jovanovich, Inc., 1978), p. 35.
8. OPSEC's subtlety is one of the reasons that it tends to be difficult. For a discussion of some other reasons, see George I. Jelen, "The Nature of OPSEC," *The OPSEC Journal*, First Edition, published by the OPSEC Professionals Society, 1993, pp. 5-8.
9. J. Thompson Strong, "Tilting with Machiavelli; Fighting Competitive Espionage in the 1990s", *International Journal of Intelligence and Counterintelligence*, Vol 7, No 2 (Summer 1994), p. 162.
10. Charles W. Butler and Norman O. Schutz, "Devising an Intelligence Collection Plan," *Security Management*, March 1993, p. 66.
11. *Protecting Corporate America's Security in the Global Economy*, (Framingham MA: American Institute for Business Research, 1992), p. 62.
12. U.S., Interagency OPSEC Support Staff, "The National OPSEC Program" by Samuel R. Raskin, *Operations Security Monograph Series*, April 1990, p. 2.

This paper by noted OPSEC expert George Jelen was originally published in *Conference Proceedings of the Fourth Annual International Security Systems Symposium and Exhibition*, Washington, DC, 16-18 November 1994., under the title, "A Rational Approach To The Management Of Declining Security Resources." It has been slightly edited to bring it up to date with recent events.