PUBLISHED BY THE INTERAGENCY OPSEC SUPPORT STAFF

THE OPSEC INDICATOR

Volume XI

Summer 2001

"Meeting The Challenges of a Changing World"

National OPSEC Conference and Exhibition Turns Up the Heat in Tampa

by Lynne M. Yates, IOSS Staff

The Westin Innisbrook in Tampa, FL was the picturesque location of the 12th National OPSEC Conference and Exhibition, June 11-15. The sprawling, lush, tropical grounds provided a scenic backdrop for the largest OPSEC conference in history — 680 professionals attended from many OPSEC disciplines including government, private industry, Federal law enforcement and others. As in the past, the conference was sponsored by the Interagency OPSEC Support Staff (IOSS) in partnership with The OPSEC Professionals Society (OPS).

IOSS Director Tom Mauriello, General Franks, and OPS President Pat Geary discuss OPSEC after General Franks' keynote address..

Registration began on Sunday afternoon in Inverness Hall and many participants arrived early to pick up their materials so they could begin reviewing the tremendous selection of courses and sessions to attend.

On Monday, the pre-conference training and seminars were held, including two full sessions of OP-300, *The OPSEC Fundamentals Course.*

More than 200 people received National Cryptologic School course credit for their participation in those sessions. The other all-day sessions were also lauded. One attendee stated that he made the trip across the country to hear Dr. Paul Moore's pre-conference session on the Chinese Intelligence Threat and was not disappointed.

The "main event" began Tuesday morning with national anthem and the MacDill Air Force Base color guard presenting the colors. The Director of the IOSS, Tom Mauriello, and the President of the OPS, Pat Geary, welcomed everyone to the conference and offered some opening remarks.

Ms. Joan Ruhl, the Deputy Chief of NSA's Defensive Information Operations Office then introduced a videotaped address from General Michael V. Hayden, Director, NSA *(see page 10 for a transcript of General Hayden's remarks.)*

Commander-in-Chief, U.S. CENTCOM Tells It Like It Is

The plenary speaker, U.S. Army General Tommy R. Franks, the Commander-in-Chief of the U.S. Central Command, offered his perspective to the current threats to U.S. interests and the growing need for operations security.

In his moving speech, General Franks stated that it is a certainty in the dangerous arena under his command (where asymmetric threats are now a reality), that some brave soldiers will no doubt die while performing operations for their country.

But, he added, he would hold himself personally responsible if he didn't use every means available, including OPSEC, to make sure that not one soldier dies unnecessarily.

General Franks spoke in detail about present threats to the United States and the problems that individuals under his

(continued on page 12)

Inside This Issue:

Identification Procedures for Thermal Transfer (TT) Cartridges and Dye Sublimation (DS) Cartridges

Follow-Up to Spring 2001 Indicator Story on Potential OPSEC Vulnerability

Step 1 - Locate fax machines, color printers, badging printers, bar-code or label printers or videoprinters.

Step 2 - Open unit where cartridges are installed.

Step 3 - Remove cartridge, if necessary, and inspect the following:

A) Is there an area of black carbon-like film stretched between the supply and take-up cavity or roll? Typically, the black film will be 8.5" wide. Some cartridges are simply rolls of black, carbon-like film.

B) For color printers, the cartridge will be a roll of multi-colored film (blue, red, yellow and black). On most of these types of printers, it is not necessary to remove the rolls for inspection. Upon opening the printer, the multi-colored film roll is easily inspected.

C) Badging printer cartridges are typically color rolls approximately 3" to 4" wide. The film roll contains color panels of blue, red, yellow, and black.

D) Bar-code or label printers typically use rolls of black, carbon-like film approximately 3" - 4" wide.

E) Video printers usually have small (approximately 4" X 6"), self-contained cartridges, that have the multi-colored panels of film.

Step 4 - If you can see a negative image on the carbon-like film, of what was previously printed on the machine, you have identified a TT or DS cartridge. (On a TT machine, the image is clear, on a DS machine, the image is faint.)

Step 5 - If you find such a printer, **you are vulnerable**. Only industrial-size shredders (such as mobile destruct shredders mounted on trucks) will adequately destroy the film transfer/dye sublimation cartridges, but the cartridges may also be burned.

Consider setting up a "Controlled Recycling" system to contain and destroy the cartridges. It should be noted, for environmental, recycling purposes, many of these cartridges can be recycled. Investigate your recycling company carefully to ensure implementation of security measures.

NOTE: If you are certain that your printer utilizes either ink-jet or laser toner technology, then your printer is not vulnerable. If in doubt, however, do the above inspection.

This article was prepared for the IOSS by Mr. Joseph R. Hurston
President/CEO of Cartridge Source of America

Director's Message

How Do You Measure Success?

When we return each year from our National OPSEC Conference and Exhibition, we can't help but wonder if the event was a success, and if it was, how to measure that success.

— If having more than a 20% increase in participants from last year's conference is a measure, then it was successful.

— If the measure is having a well-balanced selection of topics to attend, then it was successful.

— If it is having highly qualified and dynamic speakers, then it was successful.

— If it is presenting the event at a venue that is comfortable, pleasant, and conducive to learning, then it was a success.

— If it is having a conference management team that focuses on customer service and satisfaction, then it was successful.

And finally, if you have been able to partner with distinguished members of a professional organization like The OPSEC Professionals Society, then there is no doubt that you have been successful.

But the real success is what happens *after* the event. Now that the attendees are a little smarter, more informed, better trained, and have established a new network of experts in the field, it will be how they implement what they have learned that will be the true measure of the conference's success. All who attended will be receiving an electronic event critique questionnaire very soon in their E-mail. Please take the time to answer each question carefully and share your experiences with us. We will post the results in the next newsletter.

In closing, I have a word about the IOSS Bulletin on the previous page. In the last *Indicator,* we featured a story about a technical vulnerability using thermal transfer or dye sublimation cartridges in certain Fax, printer, and copy machines. As a result of the overwhelming response to that article, we have now provided a 5-step procedure to help everyone identify these machines. Remember, we are not suggesting that anyone stop using this technology; our intent is for you to simply know how to identify the cartridges and establish proper procedures for their disposal.

Enjoy the rest of the summer!

Tommy

60 Years After the Attack on Pearl Harbor – What Can We Still Learn?

by Patrick D. Weadon, NSA Historian

The 5-step process is one that has served the OPSEC community well for many years. Most of us agree that each of the 5 steps is vital. This column, however, will focus on the threat component, in the hope that by my imparting the following stark historical examples regarding the events of December 7th, 1941, you will avoid falling into the all too common habit of "believing your own press clippings."

Blame for the attack on Pearl Harbor has been attributed to many things; lack of proper reconnaissance, a focus on diplomatic rather that operational information, bureaucratic bungling at both the civilian and military command levels, etc. All of these factors played a role. However, in looking closely at the historical evidence, it becomes clear that the major reason the U.S. forces were caught unaware at Pearl Harbor was that those in positions of authority simply did not believe that the Japanese could do it. ***They did not properly analyze the threat.***

Let's examine the situation from an OPSEC perspective. At the time, those in positions of authority had no problem determining the critical information that needed to be protected. Unfortunately, when it came to considering the possibility of an attack by Japanese forces on the installation, the 5-step process came to a grinding halt at Step 1. Why design an OPSEC plan if you believe you have no opposition? Why come up with effective countermeasures when you don't think you need them?

Obviously, these observations are being given in hindsight. It is in some ways unfair to play "Monday-morning quarterback" when analyzing the infamous attack. As previously noted, many factors contributed to the debacle. However, it is ***not*** unfair (and may be enlightening) to relate the incredibly unrealistic and inaccurate view that Americans held regarding U.S. invulnerability against the Japanese Navy prior to that event. The following is a sampling of the misguided notions that influential people had concerning Japan.

"Events clearly indicate that Japan has no desire for war with the United States."

— Senator Alva Adams of Colorado,
September 1940

"Japan is moving... but we know that Japan would never move of itself against the United States..."

— House Majority Leader John W. McCormick of Massachusetts,
September 1940

"The island of Oahu, due to its fortifications, its garrison and its physical characteristics is believed to be the strongest fortress in the world...with our heavy bombers and our fine new pursuit planes, the land forces could put up such a defense that the Japanese wouldn't dare attack Hawaii."

— General George Marshall, Army Chief of Staff,
April 1941

"A Japanese attack on Hawaii is regarded as the most unlikely thing in the world, with one chance in a million of being successful. Besides having more powerful defenses than any other post under the American flag, it is protected by distance. The Japanese Fleet would have no bases from which to operate... it would have to come so far that American patrols would spot it long before it arrives...American naval men would like nothing better than to see the Japanese Fleet outside of Pearl Harbor where they could take it on."

— Clarke Beach of the Boston Globe, September 1941

"Our mission is to protect Oahu... and shipping out these Army planes will lessen our capability to do so. Why are you so worried about this?" asked Kimmel. "Do you think we are in danger of an attack?" "The Japanese have such a capability," answered Mollison cautiously. "Capability, yes" conceded Kimmel, "but possibility..." With that, he swung abruptly on Soc Morris. "What do you think about the prospects of a Japanese air attack?" "NONE, ABSOLUTELY NONE," replied the Fleet War Plans Officer."

— Exchange between Admiral Kimmel, Commander of the Pacific Fleet; Lt. Col. Jimmy Mollison, Chief of Staff, U.S. Army Air Corps, Hawaii; and Captain Charles "Soc" Morris, Fleet War Plans Officer, 26 November 1941. (Taken from the book, ***At Dawn We Slept****)*

"In the meantime, Layton joined a group of staff officers awaiting him for lunch. As he did, one of the fleet officers quipped, "Well, here comes Layton with his Saturday crisis..." Layton replied somberly, "I don't know about you, but I expect to be in my office tomorrow (Sunday, December 7, 1941)." Come off it, Layton!" one of his friends scoffed. "You said that *last* Saturday."

— Layton is Commander Edwin T. Layton, USN, Intelligence Officer for Pacific Fleet (Taken from the book, ***At Dawn We Slept****)*

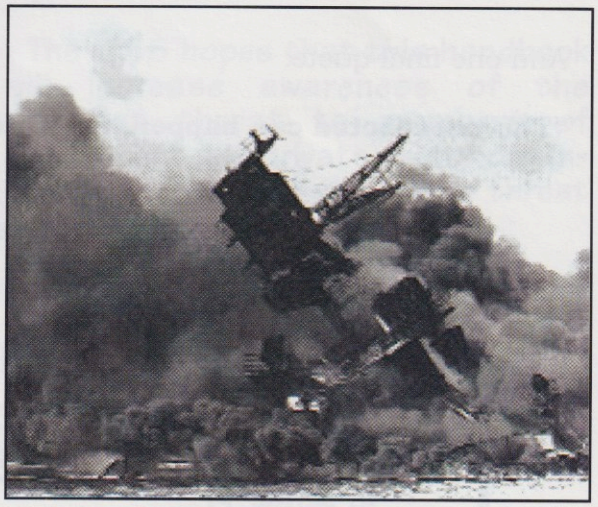
Deluding Ourselves

The astonishing fact is that both Japanese and American naval experts had been predicting for decades prior to the event that Pearl Harbor would be a likely target for the Japanese Navy. There ***were*** American experts who were wary of Japan, but their voices were in the minority.

Once again, individuals in key government positions were victims of their own prejudices and preconceived notions. Why was it that Japan was not perceived as a threat to the Pacific fleet? It was because the Americans were focusing on themselves and ***not*** on the adversary.

From an OPSEC perspective, the Americans not only failed to properly analyze the threat, they went the extra step and concluded, due to a combination of arrogance and hubris, that there ***was no threat***.

(continued on page 6)



Ablaze, the U.S.S. Arizona slips beneath the waters of Pearl Harbor — 1,177 sailors and marines died on the Arizona.

(continued from page 5)

Even after the attack, the inability to perceive Japan as a worthy adversary persisted. Some reporters of the day, not being able to bring themselves to admit that they had been wrong, opined that the Germans must have been behind the raid, because the Japanese could have never pulled it off on their own.

The Future

When analyzing the threat, never underestimate your opponents. Assume they are intelligent, motivated and, if given the chance, will come up with ingenious ways to transcend the status quo.

When Japanese Commander Minoru Genda was presented with Admiral Yamamoto's plan for a surprise attack, he did *not* say "We can't do it because our torpedoes won't work in the shallow water there," or " There is no way that we can refuel en route to the target." Rather, Genda's reply was a simple, "It would be difficult, but not impossible." Contrast this statement with the above-referenced statement given by General Marshall, and it is easy to understand why the Japanese prevailed on that dark day in American history.

It is not enough to identify what you need to protect, you must continuously apply the 5-step OPSEC process to ascertain your opponents' capabilities to act against you — and provide effective countermeasures. Above all, when you calculate the threat, have the perspicacity to see your adversaries for what they are, not what you wish them to be.

"Although the imminence of hostile action by the Japanese was known, and the capabilities of the Japanese Fleet and Air arm were recognized in war plans made to meet just such hostile actions, these factors did not reach the state of conviction in the minds of the responsible officers..."

— Secretary of the Navy James Forrestal (in the Navy's Post-Attack Report on Pearl Harbor)

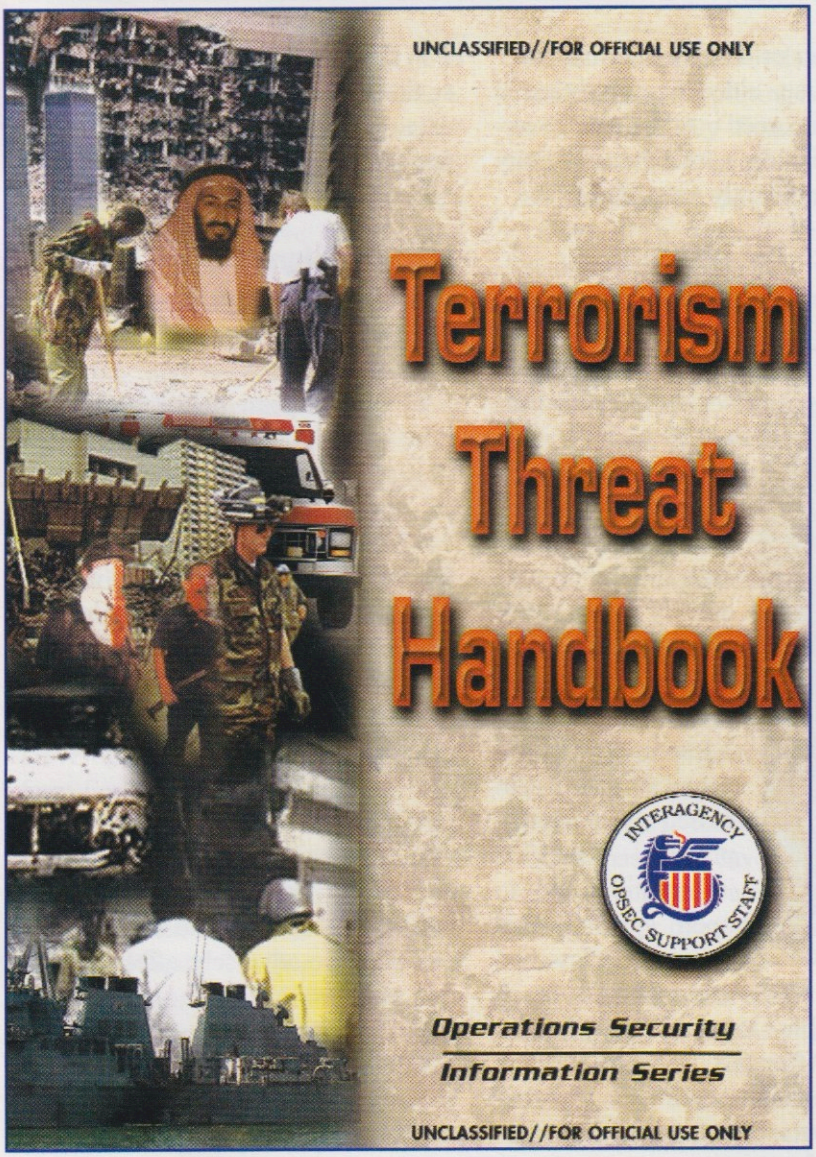
And one final quote:

"The unexpected can happen, and often does."

–Gordon Prange, Author of ***At Dawn We Slept: The Untold Story of Pearl Harbor,*** *Penguin Books, 1982."* ■

Know the Threat to Your Operations

IOSS Publishes New Terrorism Threat Handbook — A Companion to The Intelligence Threat Handbook



The IOSS is proud to announce the recent publication of the "Terrorism Threat Handbook," a companion to last year's Intelligence Threat Handbook.

This publication is designed to provide unclassified terrorist threat reference information for members of the OPSEC community .

It explains categories of terrorist threats, provides details of threats worldwide from individual terrorist groups, and identifies dates of potential terrorism significance.

Although it is based entirely on open-source reference material, it is marked "For Official Use Only" and should be protected as such.

The "Terrorism Threat Handbook" can be disseminated to authorized individuals with a national security mission.

The IOSS hopes that this handbook will increase awareness of the terrorist threat to members of government and private sector organizations and assist you in your threat assessments.

To order, simply send an E-mail to ioss@radium.ncsc.mil or send a FAX to (301) 982-2913.

Is Your Coworker A Spy?

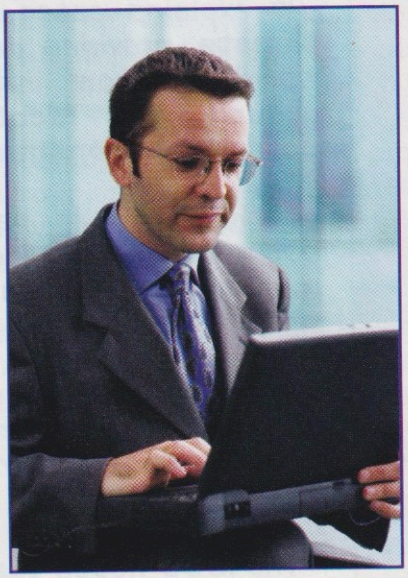
by Special Agent Chris Mariano
Informations Operations Branch, Air Force Office of Special Investigations, Andrews Air Force Base, MD

Q. Who is the greatest potential threat to Information Assurance?

A. The insider.

Anyone who has authorized access, either physical or electronic, to information and infrastructure resources, is an insider, and it's the insider who's in the strongest position to cause harm to our information systems.

Throughout history, significant problems have been created by insiders, whether acting as agents of an enemy government or simply disgruntled employees with an axe to grind.



In any case, their authorized access to information, the trust placed in them by their superiors, and their detailed, first-hand knowledge of asset value lend particular gravity to the damage they can do.

The High-Tech Workplace

Never has this been more true. Why? Because in today's high-tech workplace, enormous processing power and interconnected information systems have become commonly available.

This enables the insider to access, correlate, and associate more information from a greater number of information sources than ever before.

Insiders have the capability to disrupt interconnected information systems, to deny the use of information systems and data by other insiders, and to remove, alter or destroy information.

Even worse, aided by sophisticated and well-resourced outsiders, the severity of an insider's malicious activity may be significantly amplified.

Difficult to Detect

Making matters worse, insider misuse is harder to detect because it can operate at a higher semantic level than penetration by an outsider masquerading as an insider.

However, outsiders can also quickly attain many characteristics of an insider, making them difficult to discover.

Insider threats are posed equally to closed systems that process classified information and to open systems that process unclassified information — each is vulnerable to malicious insider action. After all, closed systems employ the same commercial off-the-shelf software and hardware components used for open systems.

The only difference, really, is the physical security, unique communications protocols, and encryption that protects communications paths and prevents interception or disruption among network components. An insider with malicious intent can cripple a closed system as effectively and quickly as an external expert can cripple an open system.

In fact, the insider may have an easier time of it, due to his or her knowledge of the systems and its controls, and the fact he or she is usually under no particular suspicion.

Warning Signs

Insider security problems arise primarily from four attitudes:

◆Maliciousness: deliberate compromise or destruction of information, or disruption of services to others.

◆Disdain for security practices: willful public display of classified information, improper storage of classified materials, improper destruction of classified or unclassified data, or the inadequate protection of classified material outside controlled facilities.

◆Carelessness: any act of disregard to the proper use of an information system or the protection of information, not necessarily meant to exploit, attack or otherwise adversely affect information systems.

◆Ignorance: lack of knowledge of security policy and practices to prevent the compromise of information.

An insider, especially one with malicious intent, has the capability to compromise America's effectiveness and place the lives of our dedicated men and women in jeopardy.

No nation has ever been able to eliminate the insider threat. The challenge is to continuously assess the threat, reduce our vulnerabilities, and seek new countermeasures. ◆

Dragontalk

Carla Colson has replaced **Pat Munson** who has moved to a new position. Carla, like Pat, is a contractor, and will maintain the IOSS database and continue to provide the high level of administrative support and customer service for which Pat was famous.

Before accepting employment with ACI, Inc. and becoming assigned to the IOSS, Carla worked for Lockheed Martin for 7 years. She says that joining the IOSS team has been a great learning experience for her. According to Carla, her favorite aspect of the job is working closely with our customers. In her spare time, Carla enjoys going to the beach and golfing.

John Glorioso the former Program Development Team leader, retired from Federal service in March.

Among his many accomplishments, John was instrumental is bringing the OPSEC and law enforcement communities together. John, who was a retired Maryland State Trooper, taught and developed numerous OPSEC courses for the National Cryptologic School for many years prior to formally joining the IOSS.

John is moving to the Maryland shore to spend more time with his family and perhaps pursue a part-time teaching position. We wish him the best in his future endeavors.

Kirby Johnson has recently joined the Survey Team. Kirby is a retired Navy cryptologic technician with 22 years of service. His Navy career began in 1968, and highlights include providing naval gunfire support during Vietnam; duty with Commander, Naval Forces, Southern Europe (NATO); and supporting Allied Forces in Bosnia. Kirby finished his Navy career in 1996 after a two-year assignment at the National Security Agency.

Kirby then worked for Electronic Data Systems (EDS), as a technical writer, providing support to the multimedia corridor contract proposal on behalf of the government of Malaysia.

In April 1998, he left EDS, and commenced his chosen career in the communications security field. Kirby enjoys working in his yard, swimming, hiking, skiing, and traveling and spending time with his family.

Gerry Mattocks is the new Program Development Team Leader and may be reached via E-mail at g.matto@radium.ncsc.mil or by phone on (301) 982-0323. Gerry, a former high school teacher and Special Agent, has been involved in OPSEC training and program development at the IOSS for more than three years.

Wayne Smith is also a member of the Survey Team. Wayne joined the IOSS in January 2001.

He retired from the Air Force after 28 years, 9 of which were spent at the National Security Agency, including a tour with NSA's Inspector General staff. He joined the DoD as a civilian in the Information Assurance directorate in 1998. After three years of customer interface and working in communications security, Wayne came on board with the IOSS survey team. He will also be augmenting the Training Team as necessary. Wayne enjoys spending time with his children and collecting beanie babies.◆

From the Editor

In the Spring edition of *The OPSEC Indicator*, we published two articles identifying OPSEC vulnerabilities. The first was a story on the potentially widespread vulnerability of cartridges in certain Fax and other common business machines and the need for these cartridges to be properly destroyed in order to protect an organization's critical information.

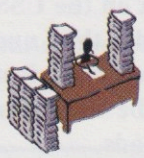
The other article related the true story of a military member discovering a chat room on the Internet for expectant military families (and the critical information that was unwittingly being revealed to a worldwide audience).

The IOSS has had more responses to these two articles than on any others previously published. Many readers requested further information on these topics to share with their organizations (see page 2 for a follow-up on the cartridge story).

This leads me to believe that there are other unclassified vulnerabilities that OPSEC professionals are discovering that could be shared in this venue to the benefit of the entire community. Please keep this in mind for future editions!

Anyone may submit articles by mail, or via E-mail to **ioss@radium.ncsc.mil,** or by Fax to (301) 982-2913. Submissions to ***The OPSEC Indicator*** are subject to editing for space, clarity and classification.

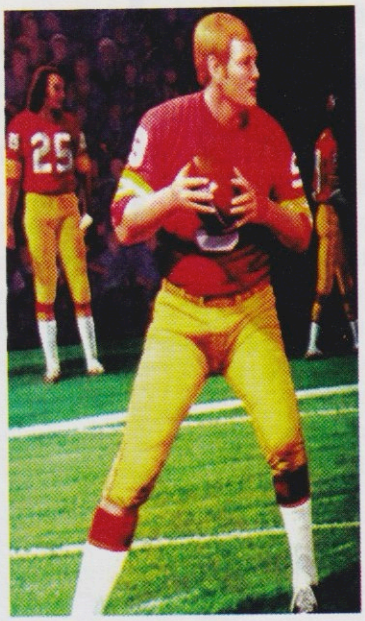
Lynne Yates



"OPSEC is Like a Good Quarterback"

NSA Director, General Michael V. Hayden's Address to National OPSEC Conference and Exhibition

"Good morning, and welcome to the 12th Annual National OPSEC Conference and Exhibition. The Interagency OPSEC Support Staff and The OPSEC Professionals Society have put together an outstanding week of programs offering a wealth of information for all of you involved in the intelligence, national security, and law enforcement communities.



There is a great deal of knowledge to be gained during this conference and I urge you to take advantage of this unique opportunity.

This morning, I want to focus on matters I believe are crucial to the future success of our Nation in confronting the threats of the 21st century - threats that are more widespread and less certain than those of the past.

As Defense Secretary Rumsfeld has said, we are now entering 'a period of continuing change, and the sooner we wrap our heads around that fact, the sooner we can get about the business of making this Nation and its citizens as safe and secure as they must be in our new National security environment.'

If we are to thrive in this continually changing environment, then we will depend on OPSEC more than ever before.

The attack on the USS Cole was a stark reminder that, under the right circumstances, American might and power can be overcome by asymmetric methods.

In the realm of national security, the rules have not only changed, they have all but disappeared.

If our Nation is to prevail in its efforts to protect its most precious secrets *and* retain the capability to protect those who stand in harms way, we *must* take a new and innovative approach to the protection of critical information.

Today, we are struggling with the reality that the marvels of the Information Age have given our adversaries the ability to attack us in ways that were inconceivable in the past.

A Hard Fought Battle

America's intelligence and defense communities are engaged in a hard fought battle to protect information that is analogous to a football game, where the standard set plays that worked so well in the past are no longer effective.

In order to defeat our opponents, we must, like a good quarterback, be prepared to issue audibles at a moment's notice.

OPSEC is versatile, and it is flexible. Used properly, it will keep our opponents guessing about our future operational planning.

More importantly, operations security forces us to consider the challenges we face on myriad levels.

It has been noted that, "Too many times in the past we have looked into the mirror of history and seen only the reflections of our own intentions."

OPSEC Fights Complacency

We need to shed the misguided notion that our adversaries think exactly like we do. Through the 5-step process, OPSEC forces us to fight off the urge to be complacent by encouraging us to think in new and different ways about the threats poised against us and about the methods and strategy we use to respond to these threats.

The Interagency OPSEC Support Staff, or IOSS, was established to promote and maintain OPSEC principles worldwide by assisting you in establishing OPSEC programs, providing OPSEC training and conducting OPSEC surveys.

The IOSS, with the help and support of The OPSEC Professionals Society, stands ready to assist you whenever and wherever you need them. This conference is only one of the many value-added OPSEC services they provide.

As you listen to the subject-matter experts and view the many interesting exhibits during this week-long conference, I urge you to think about new and innovative ways to apply the knowledge gained from this forum.

You will hear accomplished professionals discuss cutting-edge topics that will allow you to better apply the principles of operations security to your own organizations.

Topics like "Cyber Strategies, "Heat Transfer Technology," "Counterterrorism," and "Computer Network Defense" to name a few, will provide practical solutions for problems in the OPSEC realm.

In addition, Friday's classified sessions will delve into operations security-related topics such as "Communica-

tions Vulnerabilities" and "Threat Research."

Remember, these presentations have been selected because of their applicability to the daunting challenges of the current day. We sincerely hope at the conclusion of the week's events you will use what you have learned in solving your own future OPSEC challenges.

Later today, at the Annual OPSEC Awards luncheon, you will be recognizing those individuals in the OPSEC community who have found ways to apply the time-tested principles of OPSEC to real-world problems and situations such as identity theft, protection of critical technologies, OPSEC guidance for war fighting units, and others.

I am sure you join me in congratulating these winners and all who participated in this worthwhile and prestigious awards program.

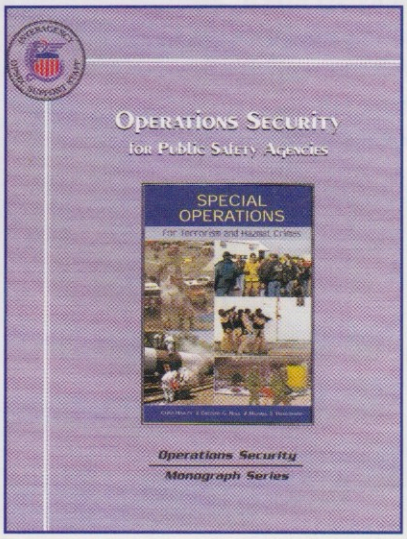
In conclusion, let us remember that the challenges of the Information Age - fingertip access to critical information and the sudden availability of high tech resources to our adversaries - will not be countered by fences and locks.

In order to prevail, we must be willing to depart from our exclusive reliance on physical security tools and utilize the tenets of the 5-step process to fire our imagination and creativity.

In short, let us never forget that OPSEC is not just theory — it is a practical, effective and time-honored analytical tool to help us keep our Nation secure."

General Hayden's schedule did not permit him to attend the conference but because of his staunch support for OPSEC, he provided this message by videotape. The message was applauded by conference attendees and was referenced by other speakers throughout the week. ◆

OPSEC Monograph Series
Summer 2001



This new publication introduces the basic concepts of establishing an OPSEC program for the public safety community and explains in detail how to apply the 5-step OPSEC process to Special Operations at the scenes of major events, violent crimes, terrorist incidents, or incidents involving weapons of mass destruction.

More and more, the IOSS is receiving requests for OPSEC training from members of the Federal public safety and law enforcement communities concerned with the potential threat of terrorist incidents in the United States.

This publication is offered in response to this growing need for information, and also focuses on incorporating OPSEC into daily planning to avoid threats to public operations.

To order, simply send an E-mail to ioss@radium.ncsc.mil or send a FAX to (301) 982-2913.

(continued from page 1)

command face on a daily basis. General Franks concluded his stirring and candid remarks by taking questions from the audience and received a standing ovation upon the conclusion of his direct and heartfelt presentation.

The conference participants had another treat in store for them on Tuesday. As usual, the Annual National OPSEC Awards were presented at the awards luncheon following the kick-off ceremony.

Perpetual Trophy

The 2001 awards luncheon began with Mr. Tom Mauriello introducing an inspirational, brief video that chronicled the extraordinary achievements of the 2001 award winners.

Award Winners

This year was the first time that the Literature Achievement Award was renamed to honor Mr. George F. Jelen, a former OPSEC manager who greatly contributed to the literature of the profession before his untimely death in 2000. Mr. Kurt Haase was awarded this prize for his fascinating treatise, "OPSEC and Identity Theft...Take It Personally!"

The multimedia award went to Federal Manufacturing and Technologies, Honeywell for their clever and entertaining series of security videos featuring fictional character Jim Leak - an engineer at an aerospace company. The high quality of the tapes and their instructional significance quickly made these indispensable OPSEC tools.

The second place award for Organizational Achievement went to the 5th Space Surveillance Squadron, Feltwell, U.K. and the first place was awarded to the 68th Information Operations Squadron, Brooks Air Force Base, Texas.

Both of these organizations revolutionized OPSEC training and procedures throughout their respective bases and solved potentially damaging OPSEC problems.

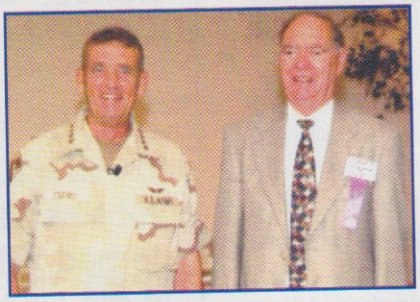
Individual Achievement

The second place award for Individual Achievement went to TSgt Michael Anthony of the 5th Space Surveillance Squadron. Along with many other accomplishments, TSgt Michael Anthony took an OPSEC program in dire need of attention and, in just six short months, transformed it into what inspectors deemed "the best OPSEC program inspected to date."

The first place award for Individual Achievement was presented to Special Agent John Fencsak of the Naval Criminal Investigative Service. Special Agent Fencsak recognized a gap in the procedures used to identify and track foreign visitors to the Naval Air Station, Patuxent River, MD.

He personally re-engineered the station's visitor program and improved its procedures for funneling key information to the Naval Criminal Investigative Service.

He also established a central database of foreign visitors to track any illicit activities and assist in identifying trends. His innovation moved decision makers to action. In response to national level requirements, numerous Intelligence Information Reports were shared with community analysts. In addition, the Department of Defense is adopting his realistic, economical plan at the national level.



Featured Speakers U.S. Army General Tommy R. Franks, Commander-in-Chief, U.S. Central Command; and Lt. General James A. Williams (retired).

OPSEC Throughout History

Following the awards presentation, retired U.S. Army General James A. "Jim" Williams delivered some remarks on the historical antecedents of operations security, with observations as to the importance of OPSEC in both government and private business.

Since his retirement from the Army, General Williams has served as a consultant and is the chairman of the board for Information Operations, Inc., a company which provides software and services to government clients in information assurance and operational capabilities as requested.

Williams entertained and informed the audience on the effective use of OPSEC during the times of Lord Nelson, George Washington, and Abraham Lincoln — all the way up to Bill Gates.

He spoke of the dangers of the Information Age and provided stark examples to prove his point. General Williams concluded by stating, "We must truly analyze our systems, our organizations, and our practices to identify vulnerabilities and then act to strengthen ourselves in those areas. How do we adjust in this changing world? How do we react to what might seem like an overwhelming set of odds?

First, take a common sense approach, and don't panic. Stay abreast of technology and use it to your advantage. Have a plan that works and then validate that plan by testing it. Correct the weaknesses you have identified and make it a continual cycle.

Ladies and gentlemen, it is not a

2001 National OPSEC Award Winners

(l to r: Mr. Tom Mauriello, Director, IOSS; Kelvin May, OPSEC Manager, of Federal Manufacturing and Technologies, Honeywell; Colonel John Raymond, of the 5th Space Surveillance Squadron; Major David Ripley, of the 68th Information Operations Squadron; Tsgt Michael Anthony, of the 5th Space Surveillance Squadron; Special Agent John Fenscak, of the Naval Criminal Investigative Service; and Mr. Kurt Haase, of the Dept. of Energy, Nevada Operations Office.)

question of 'if' but 'when' an attempt will be made against your organization or company. Will you be ready?...Who will be tagged with the ultimate responsibility? The IOSS can be your guide and mainstay — if you take it seriously and use what they teach."

Open Sessions Begin

After the luncheon, the conference began in earnest. Participants hurried to fill in the classes of their choice and many were standing room only. Layne Marino, of SecureInfo Corporation, presented a hilarious yet thought-provoking and useful session on *Marino's 10 Laws of OPSEC.*

Kevin Giblin from the Federal Bureau of Investigation gave a fascinating and sobering presentation on *The FBI's Response to Terrorism.* Among the many other topics covered on Tuesday was *Cross-Treaty Synergy* by Air Force Captain John Perez which dealt with the OPSEC problems associated with adhering to Arms Treaty regulations.

Mr. Ed Jopek, Director of Security for Veridian Corporation, teaches a session on Anti-terrorism and Force Protection, Past, Present and Future.

The Wednesday classes began with a plenary session of *"2001 - A D*I*C*E Odyssey"* by the IOSS' own Ray Semko. As usual, the Diceman brought down the house with his own brand of humor and unique insights. He also left the audience with a renewed sense of patriotism and dedication to duty and preserving the American way of life.

Following the Diceman's briefing, attendees traveled to the various buildings to attend additional informative training sessions including *FOIA, OPSEC and the Web; Caller ID, Friend or Foe?*; *Analytical Risk Management*; and Tom Mauriello's very popular *Motivation Through Communication.*

On Wednesday afternoon, the Exhibition opened with 15 booths designed to increase awareness and distribute security awareness materials and products. The exhibitors on hand were from the National Security Agency; the IOSS; the OPS; the Defense Intelligence Agency; Veridian; Security Engineered Machinery; the Defense Threat Reduction Agency; L3 Communications; the National Counterintelligence Executive Office; Infineer; Cryptek Secure Communications; Beta Analytics International; RSA Security, Inc.; and EWA/IIT Media.

Attendees network, munch, and visit exhibits during the exhibitor social.

(continued on page 14)

(continued from page 13)

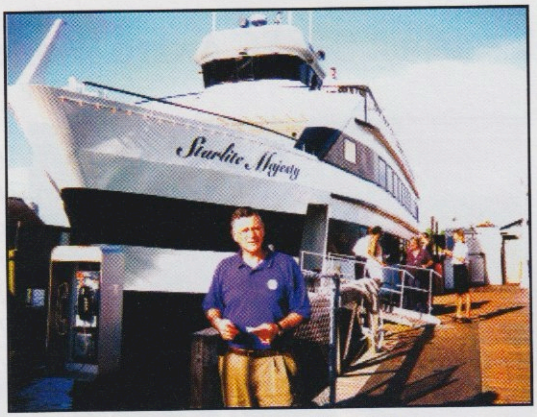
Something New

One thing different about this year's conference was that participants were given the opportunity to meet each other and network in a social setting each evening.

This change was in response to feedback from last year's conference reflecting that participants were kept so busy throughout the day that they had no time to meet and network with other OPSEC professionals.

Participants discuss technology innovations with vendor.

On Monday night, after the pre-conference seminars, the OPS sponsored a get-together in the Stirling Ballroom with light refreshments to help everyone get acquainted. On Tuesday evening, the OPS held their 10th Anniversary Dinner and Annual Meeting and all were invited to participate. After the exhibits opened on Wednesday afternoon, hundreds enjoyed a full range of hors d'ouevres and a cash bar, courtesy of the many exhibitors.



"Captain" Tom Mauriello

What many called the highlight of the week's social events occurred on Thursday evening when reservations were made for any adventurous individuals interested in a dinner cruise. Approximately 150 people enjoyed a 3-hour bay cruise with a formal dinner, live music and dancing.

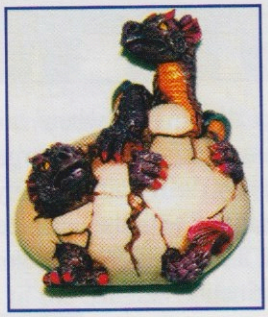
Classified Sessions

Many of the sessions on Thursday and Friday covered classified topics including *Threat Research; Communications Vulnerabilities; Profile of a Spy; and Technology and Security - Concepts of a Dangerous New World;* and were highly praised by the attendees.

Feedback

The IOSS and the OPS believed this to be the most successful conference to date and verbal feedback from the participants seemed to verify this.

The IOSS will be tabulating written critiques in hopes of addressing any future interests and further improving the conference for next year. The results of the survey will be published in the Fall edition of *The OPSEC Indicator.* ◆



Featured speakers at the conference were given the above item as a token of appreciation - it signifies the emergence of the Purple Dragon as a major force in the 21st century.

National OPSEC Conference and Exhibition Poll

In an effort to make our conference available to the largest audience possible, we would like to ask our reading public interested in attending our week-long National OPSEC Conference and Exhibition the following questions.

1. **What is the best time of year for you to be able to attend the OPSEC conference?**
2. **Where would you like to see it held?**
3. **Please provide us the name of month and week (either the first, second, third, or fourth week) for your choices.**
4. **E-mail your response to Rick Townsley of the IOSS at ioss@radium.ncsc.mil.**

Viruses Infect Palm Pilots

By Master Sgt. John Middleton
Air Mobility Command
Scott Air Force Base, Ill.

The threat posed by computer viruses is hardly late breaking news to computer users. Many people learned about them the hard way after the "Melissa" and "I Love You" viruses overwhelmed E-mail systems worldwide, causing damage estimated in billions of dollars. Now, people know. However, in the world of computer technology, new threats tend to stay one step ahead of user awareness.

Much attention is now given to the security of networks, desktops and laptops. Far less consideration is given to Personal Digital Assistants such as Palm VIIs or Blackberries. No doubt this is due in part to the fact PDAs are used far less than standard PCs. Yet, these increasingly commonplace devices are vulnerable. They will become even more so as they increase in sophistication.

Descriptions of PDA viruses used in this article were obtained from the official Symantec and McAfee anti-virus web sites.

Ironically, the relatively limited capability of current PDA models provides a degree of protection from virus infection. For example, inability to transfer attachments protects most PDAs from one common source of viral infection.

This doesn't mean PDAs are immune. In fact, there have already been reports of viruses and Trojan Horse (Trojan) programs designed to attack the Palm operating system.

"Liberty Crack" is a Trojan program aimed at PDAs that can be transferred from a host computer during synchronization.

When Liberty Crack activates, it attempts to delete applications from the PDA and reboot.

"Vapor" is another Trojan. This malicious logic causes icons to disappear from PDA screens as if deleted, though in reality they are not.

"Phage" is a PDA virus that infects applications, filling the screen with a dark gray box and causing active applications to close. Although experts consider the current risk to PDAs to be low, both the capabilities and the uses of these hand-held devices will continue to grow.

With this growth, the likelihood of a PDA downloading viruses and becoming infected will increase. Of course, viruses downloaded to a PDA from any source could also be uploaded to infect entire networks.

PDA users can protect both personal and official information by following rules that already apply to their desktops and laptops. Don't download program files or macros from any unknown, non-trusted source.

These programs and macros may include, but are not limited to, freeware and shareware.

Remember not to download freeware and shareware files without prior official written authorization.

Use government information technology resources for official government use only. This can't be repeated too often, because one common vehicle for propagating malicious logic is to hide viruses within computer games.

Theoretically, U.S. government systems should never be infected this way. However, in the security arena, theory is always dependent upon compliance.

Currently, properly configured anti-virus software must be in use on all government desktops and laptops. This will provide some protection whenever you synchronize between your PDA and PC.

Vendors are now beginning to release anti-virus software specifically for PDAs. At some point after evaluation and approval, these may be used by the government. In the meantime, immediately scanning your hard drive after uploading from a PDA is a must!

As with other types of computers, report any suspected PDA virus immediately.

With the usefulness of PDAs expanding, their popularity will probably keep pace. Increased use of PDAs will likely increase the risk of viral infection involving hand-held devices.

This risk will be mitigated only to the degree PDA users practice security. Too often in the past, meaningful security efforts have been reactive as a result of major incidents, rather than proactive. With regard to PDAs, we have a good chance to change that by starting early to address potential risks. Awareness of the PDA virus threat is the first step. ◆

National Threat Symposium & Security Awareness Fair

December 12-13, 2001

Johns Hopkins Applied Physics Lab
Laurel, MD

NEW FOR 2001 - a Two-Day Symposium!

The Interagency OPSEC Support Staff (IOSS), in partnership with the National Counterintelligence Executive (NCIX) and the Security Awareness and Education Committee, will present two days of training, briefings, and networking opportunities with a focus on operations security, intelligence threats to U.S. national security, and techniques for developing security awareness programs. Watch the IOSS and NCIX web pages for more specific scheduling information.

Wednesday, December 12 - Security Awareness Fair

The Awareness Fair is a collection of exhibits from government departments and agencies who have resources available to security professionals to assist in the development of security awareness. Many of these exhibits represent organizations who have other resources available beyond awareness issues. Information on exhibitors planning to participate will also be available on the Web in October.

Training

Five tracks will offer courses, seminars and workshops, including the IOSS' Web Content Vulnerabilities course, the Motivation Through Communications course, an SAES workshop on security awareness development, and a workshop on the organization and resources of the Intelligence Community.

Thursday, December 13 - National Threat Symposium

The purpose of the Threat Symposium is to provide the most up-to-date information available to practitioners in OPSEC, military operations, security, risk analysis, counterintelligence, and related fields, and to encourage interaction and networking within the community. A group of outstanding speakers who are expert on current intelligence threat issues facing national security will be invited for a day of briefings and discussions at the U.S. Secret level. Speakers will be selected in August 2001. Watch the IOSS and NCIX web pages for further information.

Clearances

A U.S. Secret level clearance is required to attend this event.

Fees and Registration

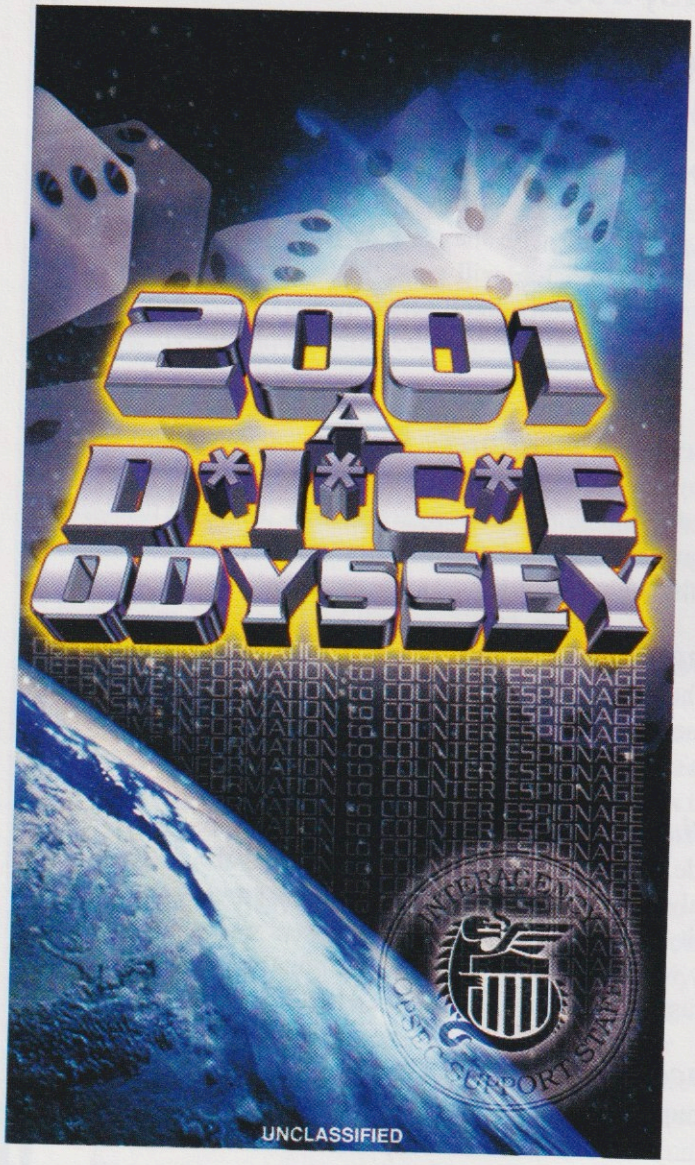
The fee is $60. Register online at ***www.iaevents.com***, or call Systematic Solutions, Inc. on 410-691-7581.

Contact Information

Call the IOSS on 301-982-0323 for additional information. E-mail inquiries can be addressed to ioss@radium.ncsc.mil. Find schedule updates at www.ioss.gov.

The D*I*C*E Man is Better Than Ever!

The IOSS Presents New Videotape of Ray Semko's 2001 Awareness Presentation



The D*I*C*E Man has been educating and entertaining audiences for more than 10 years. His briefing is unclassified but the threat information he provides is current and relevant.

From the latest espionage cases to web vulnerabilities and cyber threat, this comprehensive awareness presentation serves as a wake-up call and should be seen by everyone involved in our Nation's security.

The D*I*C*Eman's X-Files **(1999) and** ***D*I*C*E 2000 - Special Edition*** **are also still available. To order, simply send an E-mail to ioss@radium.ncsc.mil or send a FAX to (301) 982-2913.**

Protect *Your* Critical Information from Cyberterrorism

By Special Agent Daniel Fleeger
Headquarters, Air Force Office of Special Investigations, Andrews Air Force Base, MD

As our reliance on computers and information systems has grown, so has our adversaries' propensity for exploiting them to do damage.

The U.S. government has experienced a steady increase in the number of attacks against its information systems, and experts agree that the number of attacks is only going to increase.

One reason is the availability, ease of use, and sophistication of publicly available computer-attack software. Such attacks once required the skills of a computer expert. They can now be achieved by the novice computer user armed with easily obtained software.

The novice attacker is not the only threat. In general terms, computer and information systems attackers can be grouped into five major categories.

The foreign intelligence service operative is an aggressive adversary who attempts to exploit our information infrastructure for intelligence purposes. He or she can identify our members, evaluate their level of access to information of intelligence value, and even recruit their services … all in cyberspace. There are significant advantages to doing business this way, such as easily concealing one's identity, the rapidity of information flow, and plausible deniability.

The Cyberterrorist

The cyberterrorist attack goes beyond mere computer intrusions, denials of service or defacing of Web pages to actual destruction of data or systems. Use of the Internet and other information systems give terrorist groups a global and near real-time command and control communications capability. Because such groups have limited resources - and electronic intrusion can help them achieve their objectives at minimal cost - it's expected that cyberterrorism will increase. For example:

◆Organized crime targets computer systems to commit fraud, acquire and exploit proprietary information, and steal funds. Criminal organizations use electronic intrusion to hinder police investigations, collect intelligence, destroy or alter data on investigations, and monitor the activities of informants.

◆ Hackers, not too many years ago, were motivated primarily by curiosity about computer systems and network operations. In most cases, they were unlikely to engage in serious criminal activities. In contrast, today's hackers appear to be motivated by greed, revenge and politics, and their actions have become more malicious. They are more likely to aim their attacks not just at individuals, but also at enterprise information systems.

◆ The malicious insider, who has legitimate access to proprietary information and mission-critical systems, poses a significant threat because of having trusted status and familiarity with security practices.

When an insider betrays his trust, he has a much greater opportunity and ability to do harm than anyone on the outside. Moreover, he is less likely to be detected. The malicious insider, motivated by greed, revenge, or even political ideology, can act alone or with outsiders.

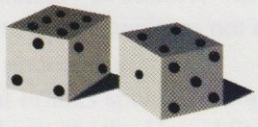
Access = Responsibility

As you can see, the threats to information systems are numerous and significant. To combat them, the U.S. government, military and contractor security offices bring to bear a number of capabilities, including defensive briefings to high-risk units and personnel, countermeasures against technical surveillance devices (or "bugs"), computer crime investigators who specialize in combating crimes against computers and information systems, and counterintelligence investigations.

But security officers can't do it alone. Everyone with access to computers and information systems is a partner in the war against cyber threats. If you detect intrusion activity, or receive unsolicited or suspicious e-mail, or discover new software or tools on your computer, or witness unescorted visitors in your work area, you should immediately contact your security officer or the local FBI.

Everyone should become familiar with the signs that an insider might be up to no good. Be wary of an insider who shows a keen interest in hacking techniques and system vulnerabilities.

Take note if an insider has configured his or her computer to provide capabilities that it shouldn't have. Other traditional indicators may be observable too, such as unexplained affluence, abnormal requests for information, and a propensity for security violations. ◆



Quarterly Quote

"Don't worry about people stealing your ideas. If your ideas are any good, you'll have to ram them down people's throats."

— Howard H. Aiken
1900-1973
Mathematician and Inventor of the
Forerunner of the Modern Digital Computer

Interagency Opsec Support Staff
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405

First Class Mail
Postage and Fees Paid
National Security Agency
Ft. Meade, MD
Permit No. G-712