PUBLISHED BY INTERAGENCY OPSEC SUPPORT STAFF

OPSEC INDICATOR

VOL.X FALL, 1999

SERVING THE OPSEC COMMUNITY SINCE 1990

Y2K is Over... And We're Still in Trouble!

By Rick Forno,
Security Officer, Network Solutions

Sometime in January 2000...

The media craze is over...No more "Century in Review" segments on the evening news, no more "gloom and doom" naysayers proclaiming the end of the world, and the MRE-Meal, Ready To-Eat will be plentiful in mail-order catalogs. Corporate and agency budgets will stabilize, and procurements will be for things other than high-priced contractor or consultant outsourcing to fix legacy systems. We survived the Millennium Bug by throwing billions and billions of dollars at the problem commonly hyped as TEOTWAWKI (The End Of The World As We Know It). We survived; everything's "business as usual," and we can now take a well-deserved break from panic procurements and last-minute fixes in the face of impending doom, right?

Wrong!

After throwing billions at the world's most expensive incident resulting from a serious lack of human foresight, the information systems that control our most critical infrastructures and services are believed to be operational come Y2K-operational, but in most cases, completely vulnerable to attack.

Why?

The Y2K Mania that skewed procurements and corporate/agency IT management focus has created a mindset that believes "if enough money is thrown at a problem, it will probably fix other problems on these systems too." Thus, the current belief is, if an organization spent $25 million on Y2K upgrades, chances are that systems security MUST have been included in that price. After all, $25 million is a hefty price tag to fix one single problem, right?

Consultants-many of them foreigners-have been paid to reprogram and upgrade hardware, firmware, embedded chips, and related technologies and software to insure things work after Y2K. Sadly, throughout the ramp-up for Y2K, a concentrated approach to systems security has been ignored-such assessments and countermeasures implementations to ensure that such systems, while operable and correctly functioning in the new year, will be indeed safe from attack or exploitation by adversaries.

Unfortunately, systems security is often viewed and planned for in a manner similar to traditional physical security: "buy it once and use it forever, because it leeches on our profit margin." Like their physical security cousins, outdated IT security implementations lead to obsolete security postures and systems that are prone to failure, compromise, or exploitation due to age or the limited resources (including people) made available to maintain and sustain them. This is a common problem resulting from management and the cultural, generational differences becoming more prevalent as we move from the Industrial Workplace to an Information Workplace.

Folks also assume that if something was purchased after 1998 (e.g., Windows NT, 98 or a new facility access-control system), it must be Y2K-compliant. President Reagan once said, "Trust but Verify" your assumptions and information. We all know what happens when we "ass-u-me" things; assumptions are proven to be the "mother of all foul-ups." For example, there are organizations just now (May 1999) receiving brand-new Windows 95-or 98-based computers or upgrades...

CONTINUED ON PAGE 4

Inside This Issue

Calendar of Events

26 October 1999	11th National Threat Symposium Laurel, Maryland
30 November-2 December 1999	Regional OPSEC Symposium Las Vegas, Nevada
5 June - 9 June 2000	National Conference Monterrey, California

For information on the above events
contact McNeil Technologies at
410-553-6465

DragonTalk

This is the inaugural edition of "DragonTalk," a new feature that will attempt in some small way to bring the OPSEC community up to speed on current events and issues in the wild and wonderful world of Operations Security.

The National Threat Symposium is slated for Thursday, 26 October 1999, at the Kossiakoff Center at the Johns Hopkins University Applied Physics Laboratory in Laurel, Maryland (also see Calendar of Events above). The IOSS staff has lined up some exciting and informative speakers on such cutting-edge topics as "Chinese Intelligence Operations" and "Adversary Use of Measurement and Signature Intelligence (MASINT)." This is a great way to get caught up with the latest and greatest in the way of threat information. More details about the Threat Symposium can be obtained from McNeil Technologies at 410-553- 6485.

For a different perspective on current OPSEC and intelligence issues, check out Michael Ignatieff's article "The Virtual Commander" from the 2 August 1999 edition of The New Yorker.

The IOSS Fiscal year 2000 Training Calendar is now available; contact the IOSS at 301-982-0323 or call 1-800-688-5115. Many of the IOSS basic and advanced OPSEC courses have been revised. New course descriptions are available; again, contact the IOSS at the above numbers.

THE DIRECTOR'S MESSAGE FALL 1999

The most significant programs that the IOSS presents each year for the OPSEC community are the annual conference and symposia. The attendees for these training and education programs have slowly reduced in number over the past few years. Those who have not taken advantage of these programs have indicated that dwindling funds have eliminated their ability to get approval from their management to attend.

An administrative change in the fiscal management of the IOSS has allowed us to make some adjustments that we trust will assist in this regard. In addition, the IOSS will also be working closely with the NSA's ISSO (Information Systems Security Organization) Corporate Marketing Support Office in the planning and presentation of our many events. Due to these changes, we have been able to reduce our registration fees significantly. We believe these initiatives will increase customer participation in the future and increase our ability to serve our customers.

I invite you to examine the new registration fees for the IOSS Regional OPSEC Symposium and the 11th National OPSEC Conference and Exhibition. The National OPSEC Conference is sponsored by the IOSS in partnership with the OPSEC Professionals Society (OPS). The fees have been reduced with no reduction in the scope and quality of these programs. You can be confident that you will experience the same first class briefings, speakers, training, and hotel/conference amenities that you have experienced in the past.

This year's National Threat Symposium will be held on Thursday, 26 October 1999, at the Kossiakoff Center at the Johns Hopkins University Applied Physics Laboratory in Laurel, Maryland. In the past, this highly attended symposium was presented free of charge to the attendees We wanted to bring the same amenities to this event that have made our other programs so successful. Therefore, a small fee has been included to provide refreshments and other logistical services necessary to make your day pleasant and fruitful. We believe that you will find this year's National Threat Symposium to be better than ever.

Letters will soon be mailed out to executive department and agency heads looking for nominations for next year's National OPSEC Awards. DO NOT wait for the bureaucracy to find you.

If you believe that your OPSEC Program deserves national recognition, then make this known to your senior management for their consideration. Remember though, nominations must come to us through your executive department/agency headquarters. If you are not sure who in your organization has received our letter-requesting nominations-just give us a call at 301-982-0323. There is an article in this newsletter that provides further details on the National OPSEC Awards Program and process. Take a moment to look it over.

In closing, may the upcoming holiday season provide you and yours with peace and joy; may the new millennium bring you new challenges and opportunities; and may the benefits of OPSEC ring strong and true in our quest for secure and effective national security operations.

Thomas P. Mauriello
Director,
Interagency OPSEC Support Staff

DragonTalk (cont)

Also in the training realm, the IOSS is currently in the process of hiring several "subject matter experts" to develop new and improved OPSEC seminars and training. The goal is to be able to offer advanced training beyond the 300 series of classes that we all have come to know and love. More info will be forthcoming on the many positive changes to our training repertoire in the *Winter* edition of *The Indicator*.

The IOSS Regional Seminar is slated for Las Vegas-that's right, Las Vegas, Nevada- from 30 November to 2 December 1999. For more information, see page 9 of this edition of *The Indicator*.

New Products! New Products! Be sure to check out the great new promotional products on page 11 of this edition.

Finally, the much-awaited year-2000 edition of the National OPSEC Conference is slated for the week of 1 June 2000 at the Naval Postgraduate School in Monterey, California. Additional information on the conference will be made available in the *Winter* edition of *The Indicator*. For now, you can get the preliminary details by dialing the McNeil Technologies number listed earlier in this edition of DragonTalk.

That's all for now. Hope to see all of you at the Threat and Regional Symposia.
PDW

Y2K is Over...(con't)

computers that, while new, are using operating systems that are not fully Y2K-compliant and will have problems during the Y2K rollover. There have even been instances of organizations spending millions upon millions installing and re-installing "new" security systems (e.g., cameras and door control devices) upon discovering these items were not ready for Y2K.

Given the pre-determined deadline of 31 December 1999 to complete Y2K upgrades, organizations have brought in anyone who can fix their systems, often at the sacrifice of strategic security foresight. Case in point: Many consultants are foreigners working on visas, or work for foreign-owned companies. Yet these people are literally given the "Keys to The Info-Kingdom" with nearly unfettered, unmonitored access to the most inner workings of our most critical systems...without undergoing anything that resembles a background check! Granted, the time to obtain clearances is considerable, but even National Agency Check or similar type commercial-sector investigations have been pushed aside in the interests of time. Everyone knows that the "insider threat" is the most common security vulnerability; so imagine the effect of a Y2K consultant with ulterior motives for working at a site...and the many secrets that could be taken from the facility completely unnoticed by security staffs.

While it's too late to start a background check for Y2K work, care must be taken to supervise and monitor these third parties in order to prevent the "insider threat" from materializing. And let us not forget Offshore Coding projects where organizations send applications out of the country for fixes. In some cases, the client (e.g., a bank) may or may not know that the "Y2K-fixit" contractor sent mission-critical code (e.g., software that coordinates bank wire transfers) to New Delhi, India, for analysis and fixing. Who checked the code when it came back to the United States for potential Trojan horses and back doors? What is the level of risk associated with this potential threat of having outsiders working on our programming code? Was it even considered in the contract negotiations? What is the pro- or anti-American sentiment in that particular country? Again, this is not often considered by IT staffs or Y2K contract managers during the rush to get things compliant.

My Y2K prediction, based on my ongoing work and future book in the field of computer incident response is this: Post-Y2K will be known as "The Year Of The Hack", and will be characterized by a considerable rise in incident response activities resulting from a large increase in computer security-related incidents, exploits, denials of service, and related attacks by those adversaries who realize the time for attack has come, knowing that many IT groups will be resting on their Post-Y2K laurels for having successfully completed a harrowing race to ensure that systems remain operational in the new year. Unless proper security safeguards and countermeasures are implemented-including proactive awareness initiatives-corporate/agency systems staff will not have much time to rest after the clocks change in December. "Year of the Rat", meet "Year of The Hack."

Recommendations

1. Start Planning Now. If you do not have proper systems security policies, procedures, and plans in place, make it happen. If necessary, outsource; but be wary of whom you outsource to. The author has developed considerable documentation and briefing materials to enable security teams to establish their own security programs and incident response capabilities in preparation for "The Year of The Hack."

2. Develop Solutions, Not Reports. Remember that processes evolve faster than policy. Ensure that your processes to combat security incidents are well known by all participants and are backed up by strong policy statements and directives. Nothing is worse than closing an incident investigation only to realize that you have not adequately addressed the underlying cause of the incident. Conducting a thorough post-mortem analysis (lessons-learned meeting) after the incident greatly facilitates the development of proactive solutions to prevent such incidents from happening in the future. Be fact-finding, not fault-finding.

3. Assume Nothing. Simply because your computer is running the "latest and greatest" operating system, do not assume it is Y2K compliant and that all applicable security fixes have been installed. Even operating systems released in 1998 were not fully Y2K-ready, and came preloaded with security vulnerabilities. As President Reagan said in the 1980s, "Trust but Verify." This goes for consultants, too...trust but verify their background through appropriate personnel investigations.

4. Network. Develop contacts in the incident response field that can assist in developing response capabilities and can provide objective, timely, and relevant information to you during a crisis. Develop methods to ascertain whether an incident is a Y2K-related systems failure or an intentional attack by an adversary.

5. Develop an Adversarial Mindset. Think like the "Bad Guy," and be proactive. Determine how to "beat" your security systems, then implement appropriate countermeasures. Not having that last quart of bubbly on New Year's 2000, or cutting back your party to be on duty in (or on call for) the network control center after midnight on 1 January 2000, may just give you the advantage of being on guard should your site come under attack. With most officers and staff at parties or on leave that night, New Year's is always a ripe time for the Bad Guy to plan an attack or incident, regardless of whether it is a cyber- or non-cyberspace (e.g., bombing) attack. Just ask the New York City Police or Fire Department how many officers are on duty during the Times Square festivities each year.

CONTINUED ON PAGE 5

Y2K is Over...(con't)

6. Out of the Box Never Works. Refuse to deploy security tools with their standard, out-of-the-box settings, including default passwords as shipped by the vendor. Most settings are either well known, or the default is set to "accept" anything. Deploy tools in a "deny all" mode; then begin to "allow" what you must, and no more. Document any and all changes to the system in order to facilitate investigations.

Through these simple recommendations-good for anytime, not just Y2K-you can help mitigate the security implications during the final months of 1999 and the Post-Y2K period, avoid negative publicity or notoriety, keep your company's stock price and employee spirits high, and help ensure the confidentiality, integrity, and availability of your information and information resources.

*Richard (Rick) Forno is a Florida native and currently the Security Officer for Network Solutions, a major internet company in Herndon, Va.

OPSEC: AN HISTORICAL PERSPECTIVE

Pearl Harbor and OPSEC

By Patrick Weadon

Gordon Prange's book *At Dawn We Slept* is considered one of the finest works on the cataclysmic events that occurred on the morning of December 7, 1941. The book provides a wonderful accounting of the events that led to the Pearl Harbor attack and gives an excellent perspective on the pre-strike maneuvering on both the American and Japanese sides.

Chapter 31, "A Significant and Ominous Change," is meant to provide some perspective on the well-designed espionage campaign carried out by Japanese diplomatic personnel in the Hawaiian Islands prior to the operation. More importantly for our purposes, the chapter also demonstrates unequivocally that the use of OPSEC by the American side could have made it much more difficult for the Japanese Imperial Navy to plan and execute the attack. Furthermore, as we shall see, Prange strongly suggests that had the United States been able to deny Japan the critical information it required to plan the attack, the members of the ruling Junta might well have felt compelled to take a different approach in their efforts to extend their empire.

It should come as no surprise that members of the Japanese diplomatic corps were engaged in intelligence gathering in the area prior to the attack. Just as today, in 1941, it was generally assumed that nation-states, particularly in times of potential conflict, would take every opportunity to learn about the capabilities of each other. However, it is one thing to conduct intelligence gathering against your potential adversary and quite another to assume that because you are both engaged in similar activities, you have nothing to fear. Unfortunately, there is strong evidence that this was indeed the attitude of the American command in the days leading up to the operation.

According to Prange, "From careful study of local newspapers and information from the Honolulu consulate, a pattern had emerged: The fleet left harbor on either Monday or Tuesdays and returned on Saturdays or Sundays. By monitoring radio traffic of American ships...the Japanese concluded that the enemy fleet customarily practiced in an area about forty-five minutes flight from Pearl Harbor...It became essential to fore-see exactly two weeks beforehand whether or not the U.S. Fleet would be in harbor on the designated day of attack."

In order to ensure that this vital information was obtained, the following "Strictly Secret" message was sent from the Japanese Naval General Staff's Intelligence Section to the Honolulu consulate requesting the following information:

"Henceforth we would like to have you make reports concerning vessels along the following lines insofar as possible:

1. The waters of Pearl Harbor are to be divided up into five sub-areas...
   - Area A. Waters between Ford Island and the Arsenal.
   - Area B. Waters adjacent to the Island south and west of Ford Island
   - Area C. East Loch.
   - Area E. West Loch and the communicating water routes.

2. With regard to warships and aircraft carriers, we would like to have you report on those at anchor (these are not so important), tied up at wharves, buoys and in docks. (Designate types and classes briefly). If possible we would like to have you make mention of the fact when there are two or more vessels along side the same wharf."

As Prange notes, this message placed an invisible grid over the harbor that enabled the planning staff to plot the position of each ship in its specific anchorage. In short, it was the information needed to formulate the bombing plan. This dispatch became famous as the "bomb plot message."

CONTINUED ON PAGE 6

Pearl Harbor and OPSEC (con't)

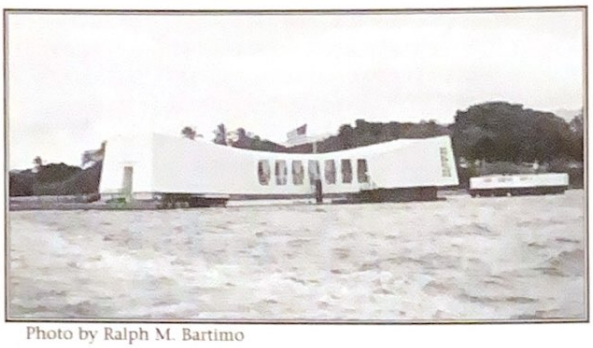

Photo by Ralph M. Bartimo

At the time of this message, the United States was intercepting and for the most part deciphering all of the diplomatic traffic sent to the consulate (the U.S. had yet to break JN-25 the Imperial Navy's code).

Col. Rufus Bratton (U.S. Army, and Chief of the Far Eastern section), upon reading the message, thought that "the Japanese were showing an unusual interest in the port at Honolulu." However, his chief, General Miles, did not consider it as anything to get excited about and "viewed it as part of the normal Japanese traffic concerning naval movements." Still troubled, Bratton routed it to the highest levels in Washington. Unfortunately, Leonard Gerow, chief of War Plans Division shared Mile's opinion and took no formal action. Perhaps the most astonishing conclusion came from Bratton's naval friends who assured him on numerous occasions that "when the emergency arises, the fleet is not going to be there, so this is a waste of time and effort on the part of the Japanese consul."

By the end of September, the consulate had gathered all the information they could from the ground. Prange notes that Yakeo Yoshikawa, one of the primary operatives for the consulate on the island of Oahu, then took his quest for intelligence literally to a new level.

"Donning his brightest aloha shirt, he took one of his geisha friends for a tourist flight over Oahu. During the trip, he could see Wheeler Field and the number and direction of runways... Military security restrictions forbade sightseeing planes to fly over Pearl Harbor," but despite this, Yoshikawa was able to clearly see the anchorage and Hickam Field. From this view he was able to estimate the number of aircraft by counting the hangars. The 20-minute flight gave an excellent view of Oahu, "firsthand experience of air conditions...where any destroyers or other craft might be cruising around... and perhaps most valuable of all, confirmed the accuracy of his observations from the ground."

It must be noted that the authorities were not totally ignorant of these kinds of activities. On the contrary, they almost expected the Japanese to try to get whatever information they could. We make a mistake in this day and age when we assume that the challenges provided by open source information are unique to this day and age. Certainly the amount of information is greater and the speed at which we can access it is much faster; however, even in 1941, open source was a problem. Witness the remarks of Commander Theodore Wilkinson, who testified at a post-attack congressional inquiry.

"We were helpless to stop it [the Japanese espionage]. We could not censor the mails; we could not censor the dispatches. We could not prevent the taking of photographs...There was nothing we could do to stop it; all hands knew espionage was going on all along and that reports were going back to Japan."

Indeed, Wilkinson's hands, like many in the defense and intelligence communities today, were tied in terms of having the ability to cut off crucial information; however, a healthy dose of OPSEC might at least have prompted the Japanese General Staff have to guess at the information or wonder if the information they were getting was accurate.

Rear Admiral Ryunosuke Kusaka, one of the major planners of the Pearl Harbor attack, wrote, "Obtaining continuous information about the enemy was one of the four major problems to be solved in executing the attack."

Prange concludes that "the cutting off of the primary source of intelligence in Hawaii might well have stiffened backbones in the Japanese Naval General Staff to the point of refusing Admiral Yamamoto, the chief architect of the raid, permission to go through with it. Yamamoto himself might have paused if he had to rely on chance and not current intelligence in order to find the fleet in Pearl Harbor."

What can the modern OPSEC practitioner learn from the lessons of Pearl Harbor? For one, OPSEC does not have to be perfect. You need only apply it to the point where, as Prange noted, your adversary is reduced to guessing.

To echo Commander Wilkinson, your adversaries will always try to get the information they need, and in many cases, due to the nature of democratic societies, you will be powerless to stop them. This is no reason, however, to throw in the towel; through the prodigious use of OPSEC you can often mitigate the damage.

Thankfully, the Japanese Naval General Staff, like the American command at Pearl Harbor, proved to be human. In the spring of 1942, Vice Admiral Seitchi Ito noted, "I felt some apprehension about Midway before it was fought...people...talked too openly about it...This was so much in contrast to the Pearl Harbor Operation and it worried me."

The very principles that allowed the Japanese Imperial Navy to prevail at Pearl Harbor (i.e., their use of OPSEC) would be conspicuously absent at Midway. This would prove to be the beginning of the undoing of Japan's westward march across the Pacific. But that is a story for another day.

CONGRATULATIONS GO TO...

YOU-YES, YOU!...

could be the next winner of a National OPSEC Achievement Award. Not only does this year's conference mark the 10th anniversary of the National OPSEC Achievement Award presentations, but it will also be the first National OPSEC Conference of the new century. Some new and exciting things are being planned for this event, and we need you to help celebrate.

The award nomination packets for the 11th National OPSEC Conference and Exhibition will be mailed soon. Make sure you read the packet carefully because some changes have been made. Nominations will be due to the IOSS Program Administrator, through the head of your department or agency, by 07 January 2000. Everyone who enters will be recognized at the Conference.

There are four categories of competition: Individual, Organizational, Multimedia, and Literature. An Interagency Awards Board will determine the winners. Thus far, the members of the Board are Ann Capitolo, Defense Threat Reduction Agency; Ellen Cronin,formally of the IOSS; Matthew Pernick, Dept. of State; and Gail Stark, OPSEC Professional Agency. For more information please call 301-982-0323.

Always Searching for Peak Performers

NEW OPSEC MANAGERS' COURSE

The Interagency OPSEC Support Staff (IOSS) will be offering a new OPSEC training course. The OP-390 course, entitled "OPSEC for Program Managers," will assist individuals assigned as OPSEC managers to acquire the tools needed to build, manage, and monitor an OPSEC program. The course has been designed to meet the needs of a program manager by familiarizing the individual with the various stages involved in developing an OPSEC program. The instructional segments combine classroom presentations, scenario-driven exercises, discussions, and a case study to assist the learner. A free exchange of information between the participants and the course facilitators is encouraged.

This pilot course will be presented at the IOSS in Greenbelt, Maryland. OPSEC program managers are requested to contact John Glorioso at 301-507-6232 or e-mail j.glorio@radium.ncsc.mil. for enrollment and course information. Each class will be limited to only 20 students in order to ensure a productive learning experience.

Eligibility: In order to attend the course, the individual must be assigned as an OPSEC program manager for a U.S. government agency, organization, or unit. In order to make the training meaningful, the OPSEC program managers will be required to forward specific information prior to class-information that will be used during different instructional modules and team exercises. The information required from the participant will be the organizational strategic plan, OPSEC policy, and Table of Organization from his/her organization.

11TH ANNUAL NATIONAL THREAT SYMPOSIUM

"EMERGING THREATS TO NATIONAL SECURITY"

26 OCTOBER 1999
KOSSIAKOFF CENTER
THE JOHNS HOPKINS UNIVERSITY
APPLIED PHYSICS LABORATORY
LAUREL, MARYLAND

FOR INFORMATION CONTACT
MCNEIL TECHNOLOGIES AT
410-553-6465

SPONSORED BY THE INTERAGENCY OPSEC SUPPORT STAFF

Sponsored by
The Interagency OPSEC Support Staff (IOSS)

Hosted by
Department of Energy (DOE)/Nevada Operations Office

For additional information,
please call McNeil Technologies at (410) 553-6476
or send an e-mail tjo opsec@mcneiltechmd.com.