

OPERATIONS SECURITY PROFESSIONALS: ENABLING CRITICAL INFORMATION IDENTIFICATION, VULNERABILITY, ANALYSIS & RISK MANAGEMENT

The Operations Security Professionals Society, P. O. Box 150515, Alexandria, VA 22315-0515
www.OPSECSociety.org

A Message from our President

Daryl Haegley

Advice for May 2009: Attend the National OPSEC Conference; Go Forth and Multiply OPSEC!

Each year hundreds flock to the National OPSEC Conference to network with fellow practitioners, mind-meld with the experts and generally have a memorable learning experience. Despite changing times, some constants remain - like the true essence of OPSEC. Direct from the "Father of Modern Day OPSEC," Mr. Robert (Sam) Fisher authored the following in May, 1990, but it still applies today:

"The objective of OPSEC is to enhance the effectiveness of our operations. OPSEC is not a substitute for sound counterintelligence and security programs; further, it is not a panacea for all information protection problems.

The ideal OPSEC practitioner should have the skills of operations, intelligence, and security analysts. Obviously, that is rather a rare bird; only a few have been sighted. From a practical standpoint, however, the practitioner need not be expert in all disciplines, but he must be aware of them and have access to experts. Given a classified or sensitive operation, program, or function, the OPSEC practitioner must:

- understand the goals and objectives of management;
- aid management to identify critically important information, i.e., information which an adversary must acquire to inhibit or stop attainment of those goals and objectives (or achieve his goals and objectives);
- identify work processes and information flow;
- identify the practices and procedures that are susceptible to adversary exploitation and which, if exploited, would disclose information deemed critically important;
- estimate the adversary's capability, opportunity, and motivation to exploit specific practices and procedures;
- assess the relative significance of specific threats and vulnerabilities;

INSIDE THIS ISSUE

A Message from Our President	1
Board of Directors	2
OPSEC Professional Society – Committees	2
Joint Reception	3
OPSEC Committee News	4
National OPSEC Conference Scoop	5
NSI's Security NewsWatch	7

- aid management in devising and implementing actions to degrade or eliminate adversary or competitor collection and exploitation capabilities; and,
- aid management to eliminate exploitable weaknesses by means of policies, procedures, hardware, and software."

This conference provides a means to learn and apply OPSEC through new ideas and fresh contacts. OPS is over 300 members strong, provides access to legacies like Mr. Fisher and has a high caliber professional certification program that is becoming the gold standard.

A number of OPS members will be speaking at the conference. At each track, at the workshops as well as those mentoring aspiring OPSEC Program Managers during the week. To enable networking, OPS members can meet together each day between 1700-1800 in the Speaker's Room.

Aiding the Interagency OPSEC Support Staff facilitate the conference, OPS members will be volunteering as Moderators and Monitors. Moderators introduce speakers at the beginning of the presentation and Moderators will ensure everyone attending has a badge, and then counts the number of attendees, relaying that number to the IOSS staff. Those wanting to volunteer please meet with the IOSS staff at 1600 on Sunday, May 10, 2009, at the Convention Center (if not arriving until Monday, May 11, 2009, an attending OPS rep will relay the information at 1700 on Monday, May 11, 2009, in the Speakers Room).

Take the time to interact with other attendees and listen and learn from them. It's easy to sit or stand alone, but I challenge you to find at least five new friends then stay

in touch with them after the conference. Come by the OPS booth to pick up your OPS Member ribbon and proudly wear it on your event badge. Make us one of your five new friends - and maybe win a prize!

Sincerely,

Daryl Haegley, OCP, CCO
14th National President
Board of Directors
OPSEC Professionals Society
Email: president@opsecsociety.org
Web: www.opsecsociety.org

Board of Directors

Daryl Haegley, President
Email: President@OPSECsociety.org

Larry Pugliese, Vice President, Chair of Revenue Committee
Email: Merchandise@OPSECSociety.org

Linda Roseboro, OCP, Secretary
Email: Secretary@OPSECsociety.org

Karen Titherington, Treasurer
Treasurer@OPSECSociety.org

Lowell Little, OCP, Board Member, Speakers Project Lead

Amanda Giovanni, Board Member, Chair of Membership & Communications Committees, Editor, OPSEC Newsletter
Email: Memberships@OPSECsociety.org

Janice Edwards, Board Member
Deputy Chair of Membership & Communications Committees

Pat Hyland, OAP, Board Member, Chair of Education Committee
Education@OPSECSociety.org

Joe Saul, OCP, Chair of the Standards Committee
Certifications@OPSECSociety.org

J. J. Mick Mickelson, OAP, Member of Membership & Communications Committees

Bill Johnston, Member of the Original Purple Dragon Team, Special Assistant to the President

Board of Directors (cont)

Victor “Top” Watson, Member of Membership & Communications Committee and MOP Administrator
Email: MembersOnlyPortal@gmail.com

Carla Gregor, Executive Assistant to the Board of Directors and Member of Membership & Communications Committee
Communications@OPSECSociety.org

OPSEC Committees

Membership: Duties include to receive and process applications for membership, to decide on eligibility of prospective members subject to the review and judgment of the Board of Directors and to promote the increase of Society membership. If you are interested in this committee, please contact Amanda Giovanni at Memberships@OPSECsociety.org

Finance: Duties include to verify all Society assets and liabilities, examine all records of the Treasurer to insure that standard, basic accounting procedures are being used, insure that bills are being paid promptly and fully identify the material or service provided, at or near year-end, review expenditures in relationship to the Annual Budget and make recommendations for the next year’s budget plan and examine such other records as the Committee Chairman might deem necessary. If you are interested in this committee, please contact Karen Titherington at Treasurer@OPSECsociety.org.

Education: Duties include develop and oversee the production and execution of programs and seminars of interest to the membership, as well as educational programs for the benefit of government agencies and private sector corporations. If you are interested in this committee, please contact Pat Hyland at Education@OPSECsociety.org.

Professional Standards: Duties include to define the terms of reference used in or relative to the practice of Operations Security, to develop the standards of training, education, and professional experience to evaluate and provide for certification of OPSEC professionals, to develop such other standards and qualifications as the Board of Directors might direct, and administer the professional certification process under Board of Directors approved procedures. If you are interested in this committee, please contact Joe Saul at Certifications@OPSECsociety.org.



SARMA, OPS and OSPA to Co-Host Reception at 2009 National OPSEC Conference

Marking yet another step in a growing partnership, the Security Analysis and Risk Management Association (SARMA), OPSEC Professionals Society (OPS), and Operations Security Professional's Association (OSPA) will co-host a joint reception at the upcoming National OPSEC Conference in San Antonio, TX. The reception, which will be held on the evening of Tuesday, May 12, 2009, is open to all conference attendees free of charge. The event will be attended by leaders from all three organizations, including SARMA Board Chair Phil Lacombe, OPS President Daryl Haegley, and OSPA President Christopher Cox. There will also be complimentary hors d'œuvres and a cash bar.

"This is an exciting opportunity to continue our efforts to build bridges between the various elements of the security risk management community," said SARMA President Kerry Thomas. "Such events allow us to develop the types of partnerships necessary to grow and mature the profession, and we are delighted to join with OPS and OSPA in holding this reception."

"Each organization serves as a means of educating and resourcing OPSEC and Risk Management practitioners," claims Daryl Haegley, President of the OPSEC Professionals Society. "A combined reception enables immediate networking and future collaboration, resulting in an expanded body of knowledge and united forces best prepared toward maintaining a strong national defense."

"OSPA, OPS and SARMA are three world-class organizations with the same goal- to see security implemented in all walks of life, from the soldier in the trenches, to the teacher in the classroom, to the police officer on the beat," says OSPA President, Chris Cox. "I'm pleased to see these resources being pooled for such a greater good, and look forward to seeing what we can do when we work together".

***Joint SARMA, OPS, OSPA Reception
Grand Hyatt, Bowie B
6:00pm – 8:00pm
Tuesday, May 12, 2009***

OPSEC Committee News

Revenue

Larry Pugliese, Chair, OPS Revenue Committee
and Vice President, OPS

New Merchandise!!

Are you interested in purchasing OPS merchandise? The OPS Revenue Committee is charged with generating revenue for the society primarily through sales of OPS merchandise. New and exciting items will be available for purchase at the 2009 National OPSEC Conference. Visit the OPS Booth to see what's available for purchase. Included are OPS Logo Polo Shirts and OPS Logo Button-up Denim Shirts, to name a few.

OPS Coin Design Contest

The contest is now over and a winning design has been chosen. Congratulations to **Mr. August Shellhasse** for winning the contest. Mr. Shellhasse's coin will be unveiled at the National OPSEC Conference and will be available for purchase after the conference on the OPS Website.

A panel of three judges comprised of the OPS Board of Directors decided on the best design based on the following criteria: Creativity – 50%; Relevance to OPSEC – 25%; Relevance to OPS – 25%. The entry with the highest cumulative score was chosen. I would like to give Honorable Mention to all of the individuals who submitted designs: Mr. Pennington Smith Jr., Ms. Priscilla Godbee, Mr. Dale De La Porte, Ms. Jennifer Bevins, Mr. Joel Leopard, and Ms. Kelli Cagle.

As First Place winner, Mr. Shellehasse will be awarded an OPS Logo Polo Shirt of his choice plus a coin with the winning design. Honorable mention recipients will be awarded a coin with the winning design.

Check the OPS Merchandise website after the Conference for new items. And if you are attending the conference in May, stop by the OPS Booth! Hope to see you there!

Professional Standards

Pat Pattakos

To promote uniformity in promoting and applying standards for OPSEC professionals, the Board of Directors has established a permanent committee that will concurrently function to establish/maintain OPS professional standards and as the panel for reviewing all applications for OPSEC Certified Professionals (OCP) and for OPSEC Associate Professionals (OAP). In the past, the OCP/OAP panel membership was rotated among OCPs but this was found to be cumbersome and led to inconsistent results. The committee membership presently consists of three former presidents and a former vice president of the society all of whom are OCPs. The chair is Joe Saul and members are Bill Feidl, Pat Geary, and Arion (Pat) Pattakos.

The committee has drafted revisions to the contents of the OCP/OAP application for more clarity and agreed to voting and review procedures. The finalized refinements have been posted to the Society's web page (www.opsec.org). The committee members have pledged to review and advise applicants of the status of their properly completed applications within two months of their receipt. Of course, this depends on the applicants completing his/her application completely and accurately. A new certificate has been created to recognize the award of the OCP/OAP designation.

Given the increased emphasis on OPSEC, it makes sense to take this important step for recognition as an OPSEC professional. All who are qualified are encouraged to apply. The committee looks forward to evaluating your contributions to our profession and taking prompt action in light of those contributions. Our policy for successful candidates is to advise supervisors of this significant accomplishment when they are identified as a new OCP/OAP.



The 2009 National OPSEC Conference Scoop

The Interagency OPSEC Support Staff (IOSS) is pleased to be joining forces with the Joint OPSEC Support Center in holding the 2009 National OPSEC Conference at the Henry B. Gonzalez Convention Center in San Antonio, Texas, this year! Here are a few highlights you can look forward to.

- We have invited over 50 presenters to speak on topics ranging from “Applying OPSEC in a High Threat Environment” to “What to Look For in a Document Review” to “OPSEC For the Younger Generation.” All of these presenters are experts in their fields. They are enthusiastic about Operations Security and willing to share their expertise with you! We are very excited to offer a session called, “OPSEC in the Field” which will highlight military and civilian personnel who have recently been deployed to various locations worldwide. These folks will talk about their OPSEC experiences in Iraq, Afghanistan, and Honduras.
- Are you a new OPSEC Program Manager or one who needs to revitalize an existing program? You should consider applying to the **OPSEC Program Managers Tutorial!** The program requires a few hours each day of the conference week and there is no additional cost to participate in this activity. Based on the IOSS Associates Program, it is intended to provide an opportunity for program managers to work with IOSS and other organizational mentors to develop materials they will use in their own organization’s OPSEC programs. Participants who complete the tutorial will receive a CD of special briefings and other materials to assist with their OPSEC program manager responsibilities. Seating is limited but you can contact Mr. Scott Milliman on 443-479-4734 or email him s.millim@radium.ncsc.mil for more details and registration requirements and prerequisites.
- There are various societies and associations who have close ties with the Interagency OPSEC Support Staff. These groups will be attending the conference and have exhibit booths available for you to visit and discuss OPSEC issues.
- The networking opportunities at the National OPSEC Conference are unlimited. We expect over 800 OPSEC professionals to attend this event. You will be able to share your experiences and lessons learned with a group of kindred spirits who are all working toward the same goal as you – a more secure organization, society and nation.

Featured Topic and Speaker:

Mr. Ron Olive has spoken at two previous OPSEC conferences (2006 in Dallas and 2005 in San Diego) and was such a big hit, that we wanted to invite him back for an encore.

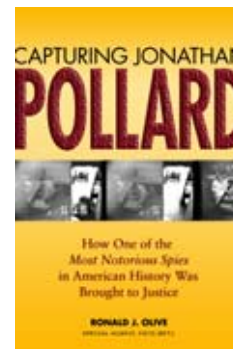
Breakdown of National and Organization Security - The Pollard Case

Jonathan Jay Pollard, an intelligence analyst working in the U.S. Naval Investigative Service’s Anti-Terrorist Alert Center, systematically took highly sensitive security secrets from almost every major intelligence-gathering agency in the United States.

Over the course of 18 months in the mid 1980s, Pollard stole and subsequently sold to Israel more than one million pages of highly classified material - enough to fill a six-by-ten-foot room stacked six feet high. No other spy in the history of the United States has stolen so many secrets, so highly classified, in such a short period of time. Ronald J. Olive was the assistant special agent in charge of counterintelligence in the Washington office of the Naval Investigative Service who led the whirlwind investigation against Pollard. Olive interrogated Pollard and garnered the confession that led to his arrest in November 1985 and eventual life sentence.

During the 20 plus years that Pollard has spent in prison, many questions have arisen about the case because it never went to trial and so much information surrounding it remains classified. Most of the books and articles that have been written about Pollard denounce his life sentence as unjust.

This lecture tells the other side of the story. It is an account from deep inside the espionage investigation that gives details of Pollard's early years and how he could have been stopped before causing extremely grave damage to our national security. Also revealed is Pollard's confession immediately following his arrest and describes Pollard's interaction with Olive before and during the time suspicion about his activities was mounting.



Mr. Olive hopes the vital insights his book offers will serve as a lesson in history, recognize similar security problems occurring now within government and corporate America, and provide an antidote to the uncertainty that has fueled speculation, rumor, and lies surrounding the Pollard case.

Mr. Olive will be available during the conference to sign copies of his new book *Capturing Jonathan Pollard - How One of the Most Notorious Spies in American History Was Brought To Justice*.

Mr. Ronald Olive began his career serving five years in the U.S. Marine Corps. While assigned to 3rd Reconnaissance Battalion, he was awarded the Bronze Star with combat "V" for valor in the former Republic of South Vietnam. He attained his master's degree in Administration of Justice and spent 30 years in law enforcement, the last 22 with the Naval Criminal Investigative Service (NCIS), mostly in foreign counterintelligence (CI).

As a special agent, he worked criminal, CI investigations, counterespionage special operations, terrorist issues overseas and in the United States, and held senior management positions in the Washington, DC, area. During this period of time, Mr. Olive was the assistant special agent in charge of CI and led the whirlwind investigation of Jonathan Jay Pollard and garnered his confession of spying against the United States for Israel.

Upon retirement from NCIS in 1999, he became the first recipient to receive the Counterintelligence Career Achievement Award. He authored the book, "Capturing Jonathan Pollard- How One of the Most Notorious Spies in American History Was Brought to Justice," published by Naval Institute Press.

He now runs his own consulting and confidential investigations company near Phoenix, Arizona. Mr. Olive is a certified Department of Energy instructor and is contracted part-time to present counterintelligence briefings with the Counterintelligence Training Department. He also works part time with the National Center for Missing and Exploited Children, "Team Adam"- Missing Child Rapid Response System.

- If you suddenly discover that you cannot attend the Conference this year, please go to www.nsa.gov and cancel your registration – this will allow someone from the waitlist to attend. If possible please cancel at least 5 working days (preferably more) prior to the event so the waitlist person will have time to organize travel, hotels, etc. We don't want to have anyone on the waitlist this year!

If you have any questions, please don't hesitate to email me or call me on 410-854-3354.

Linda Heaton
IOSS Event Coordinator

National Security Institute's Security NewsWatch

April 14, 2009

Welcome to NSI Security NewsWatch, a roundup of news, trends and issues of concern for busy security professionals. This complimentary news service is distributed twice each month. Sign up to get your own copy at <http://nsi.org/newswatch.html>

In this issue

- Report: Cyberspace remains a dangerous frontier
- Despite downturn, IT security spending to increase
- President's cybersecurity review covers a lot of ground
- Egypt Arrests 49 In Planned Attacks
- Chinese man in US accused of trade secret theft
- Infamous spy's son released pending trial
- Pentagon preps for economic warfare
- 12 Arrested In Very Serious Terror Plot In UK
- Security-Clearance Checks for OPM Allegedly Falsified
- Electricity Grid in U.S. Penetrated By Spies
- Growing threat from cyber attacks: US general
- PowerPoint security bug found in Office 2003

Report: Cyberspace remains a dangerous frontier
(GCN, 4/14/09)

The number of compromised computers actively being used in botnets to launch attacks on any given day last year was about 75,000, according to a new report on Internet threats from security firm Symantec Corp. The figures appear in Symantec's 2008 Government Internet Security Threat Report, culled from the company's broader annual Internet threat report. Data for the reports were gathered from Symantec's global network of 250,000 network sensors.

The report paints a picture of a fluid world in which people who launch attacks - which can include hackers, as well as organized criminal syndicates and possibly even nation-states using their services - adapt to changing conditions to stay at least a step ahead of security companies and law enforcement. [More](#)

Despite downturn, IT security spending to increase
(SC Mag., 4/13/09)

Management increasingly is recognizing security as a top business priority, which is resulting in higher budgets for some organizations despite the economic slowdown, according to a new survey. The survey from the Computer Technology Industry Association (CompTIA), an IT trade group, compiled the responses of 1,538 organizations of varying sizes in the United, Canada, India, UK and China. According to the survey,

regardless of region, the mean spending for security-related technologies now is \$719,930, an increase of 20 percent compared to last year.

Forty percent of organizations said they will spend more on security technologies this year and 32 percent will spend more on security training, the survey concluded. Another 33 percent will increase spending on security-related processes and 21 percent will allocate more cash for certifications, according to the survey. Spending decreases in these areas are only expected to happen in about four percent of organizations. [More](#)

President's cybersecurity review covers a lot of ground, but doesn't plow deeply (GCN, 4/13/09)

The 60-day review of the country's cybersecurity posture that President Barack Obama ordered in February is expected to be wrapped up this week. So far, the effort has received good reviews, but do not expect it to result in a detailed road map for securing our information infrastructure. The results will yield a high-level strategic plan that just scratches the surface of the challenges we face, administration officials said in a background briefing on the project.

But a critical question about cybersecurity policy that has frustrated officials in government and the private sector for years has been answered. That question was: Who's in charge? The answer is: the White House. It will be up to agencies to execute the plans, but the White House will be the anchor for policy going forward, the officials said. [More](#)

Egypt Arrests 49 In Planned Attacks
(WSJ, 4/13/09)

Egypt said it has cracked a major Hezbollah network operating within its borders, in a sign the confrontation in the Mideast between U.S. allies and more radical forces aligned with Iran is intensifying. In recent days, Egyptian authorities have said 49 Hezbollah members and sympathizers were arrested on Egyptian soil between November and January. Led by a Lebanese man known as Sami Shihab, they are suspected of smuggling weapons and ammunition, plotting attacks, and spying, Egyptian officials said.

The long-simmering hostility between Hezbollah, the Lebanese Shiite movement with a powerful military wing whose main sponsor is Iran, and the Egyptian government flared up in January during Israel's

assault on the Gaza Strip. Egypt kept its border with Gaza closed and refused to help Hamas, the Palestinian Islamist movement that governs the strip. The U.S. classifies both Hamas and Hezbollah as terrorist organizations. [More](#)

Chinese man in US accused of trade secret theft (Business Week, 4/10/09)

A Chinese national living in the United States has been accused of stealing a software program from his former U.S. employer and selling a modified version to the Chinese government after being fired. Yan Zhu, 31, a resident of Lodi, was arrested for stealing programming-source code needed to modify the encrypted program as well as internal sales materials from the company, the FBI said.

Authorities would not name the company or identify its corporate headquarters, saying only that it is located in Mercer County, New Jersey. He and two conspirators sold the program to environmental protection agencies in China's Hebei and Shanxi provinces for about 10 percent of its \$1.5 million value, according to the FBI. [More](#)

Infamous spy's son released pending trial (CNN.com, 4/10/09)

The son of an infamous CIA double agent who is himself accused of spying was released from jail last week in Portland, Oregon, pending trial after a federal judge ruled he did not pose a flight risk. Judge Anna J. Brown ordered that Nathaniel Nicholson, 24, can be freed provided he stay with family, not leave Oregon without permission from authorities and wear a GPS monitoring device.

Brown also ordered that he not have any contact with his father, the admitted spy Harold James "Jim" Nicholson. The elder Nicholson pleaded guilty in 1997 to spying for Russia and is the highest ranking CIA officer ever to be sentenced for espionage. While serving a 23-year prison sentence, prosecutors allege, Jim Nicholson, 58, restarted his career as a double agent and enlisted his son Nathaniel in his efforts to collect money owed to him by the Russian spy services and to sell more secrets. [More](#)

Pentagon preps for economic warfare (Politico.com, 4/9/09)

The Pentagon sponsored a first-of-its-kind war game last month focused not on bullets and bombs - but on how hostile nations might seek to cripple the U.S. economy, a scenario made all the more real by the global financial crisis. The two-day event near Ft. Meade, Maryland, had all the earmarks of a regular war

game. Participants sat along a V-shaped set of desks beneath an enormous wall of video monitors displaying economic data, according to the accounts of three participants.

But instead of military brass plotting America's defense, it was hedge-fund managers, professors and executives from at least one investment bank, UBS - all invited by the Pentagon to play out global scenarios that could shift the balance of power between the world's leading economies. Their efforts were carefully observed and recorded by uniformed military officers and members of the U.S. intelligence community. [More](#)

12 Arrested In Very Serious Terror Plot In UK (CNN.com, 4/9/09)

British police recently arrested 12 people in a counterterrorism operation, and locations were being searched, authorities said. Arrests were carried out in a series of raids in northwest England, police said. The men arrested were involved in a "very serious" plot closely associated with al Qaeda and escaped al Qaeda operative Rashid Rauf, whom British intelligence have linked to the 2006 plot to blow up trans-Atlantic airliners, according to a security source with knowledge of the investigation.

The new plot was not believed to be targeting national infrastructure, such as rail lines, airports or utilities, nor was it clear if the plot was to involve bombs or an assault involving gunmen, the source said. Details, the source said, were speculative at this point in the investigation. The source also said authorities don't believe the targets would have been in the north of England, where the arrests took place, and that at least some of those arrested were Pakistanis in the United Kingdom on student visas. [More](#)

Security-Clearance Checks For OPM Allegedly Falsified (Wash. Post, 4/9/09)

Half a dozen investigators conducting security-clearance checks for the federal government have been accused of lying in the reports they submitted to the Office of Personnel Management, which handles about 90 percent of the background inquiries for more than 100 agencies.

Federal authorities said they do not think that anyone who did not deserve a job or security clearance received one or that investigators intentionally helped people slip through the screening. Instead, law enforcement officials said, the investigators lied about interviews they never conducted because they were overworked, cutting corners, trying to impress their bosses or, in the case of one contractor, seeking to earn more money by racing through the checks. [More](#)

Losses Mount as Security Risks Rise and IT Struggles (esj.com, 3/23/09)

Security risks are real and growing, and they'll continue rising for at least the next two years, according to IT security professionals interviewed for Symantec's recent report, *Managed Security in the Enterprise*. Other key findings of the survey of IT security risks, challenges, and strategies: managers say it's getting harder for them to provide effective IT security because of increased regulatory pressures, a smaller budget, and problems finding and hiring qualified staff.

Organizations reported increased threats and a rise in actual attacks in the last two years; respondents expect the trend to continue in the next two. Actual losses (including lost revenue and lost staff productivity) were reported by virtually all (98 percent) enterprises surveyed. In fact, 88 percent of U.S. organizations reported being attacked in the last two years, of which 42 percent saw attacks on a regular basis. [More](#)

Growing threat from cyber attacks: US general (AFP, 4/7/09)

Cyber attacks pose an increasingly serious and costly threat to US government and commercial networks, a US general warned. The attacks range from relatively simple attempts by teenagers to highly sophisticated cyber assaults, General John Davis, deputy commander of the joint task force for global operations. Although there were safeguards for military networks, attacks on commercial networks also were cause for concern, Davis said.

"Even the indirect threat is of concern to us because a lot of our systems in the military ride over the commercial infrastructure," he said. The Pentagon several months ago was faced with "a particular worm that was concerning us that intruded into our military networks, Davis said. Last year the Defense Department prohibited the use of external computer flash drives to counter a virus threat. The Defense Department spent more than

100 million dollars in the past six months repairing the damage done by the cyber attacks. [More](#)

PowerPoint security bug found in Office 2003 (GCN, 4/6/09)

A new zero-day remote code execution vulnerability has come to light, this time affecting Microsoft Office PowerPoint. The software giant has issued a security advisory about the potential exploit, which affects older Microsoft Office versions up through Office 2003. The current flagship Office 2007 product is not vulnerable.

Microsoft said it is only "aware of limited and targeted attacks that attempt to use this vulnerability." Users with fewer administrative rights could be less affected than those who have superuser or carte blanche access to enterprise systems, according to Redmond. The attacks are triggered by getting users to click on a malicious Office file, either on a Web site or via an e-mail attachment, triggering malware on the user's workstation. [More](#)

TO LEARN MORE ABOUT ADVERTISING AND SPONSORSHIP OPPORTUNITIES;

TO MAKE A DONATION;

TO SUBMIT INFORMATION ABOUT AN UPCOMING EVENT;

INTERESTED IN SUBMITTING AN ARTICLE TO THE OPSEC NEWSLETTER – SEND YOUR PROPOSED ARTICLE TO AMANDA GIOVANNI:

EMAIL: Amanda Giovanni at Memberships@OPSECSociety.org or call 703-922-8775.

Keep Getting This Newsletter

To ensure delivery to your inbox (not bulk or junk folders), please add Communications@OPSECSociety.org to your address book.

TO SUBSCRIBE: If you were sent this by a colleague and wish to subscribe to OPSEC Society's complementary Risk Management in Action e-newsletter, please send an email to Communications@OPSECSociety.org

TO UNSUBSCRIBE: This news service comes to you from the news team at the OPSEC Society. If you do not wish to receive it in the future, please reply to this e-mail with the subject line "Un-subscribe."

Please feel free to share this e-mail with your colleagues and encourage them to sign up to get their own copy at Communications@OPSECSociety.org