



The OPSEC Professional Society - Risk Management in Action

Operations Security Professionals: The Keys to Risk Management
in a World of Increasing Risks

OPS News - 01 October 2008

NOTE: OPS MEMBERS: This is the first publication of the revamped OPS NEWS that is one of your benefits. Below are publications from informative partners that promote topics pertinent to the OPSEC community, *LUBRINCO* and *National Security Institute*. After a review of several options to replace the prior recurring products, these are not only more relevant, but save OPS members \$3,600 annually. If you know of similar products, please send the information via email to: Communications@OPSECSOCIETY.ORG Thanks to Daryl Haegely, OCP, our Vice President, for instituting this product. He is at: VicePresident@OPSECSOCIETY.ORG

We recently had the honor of hosting **Bill Johnston, Purple Dragon** at the Advanced Sensor Technologies PSO Conference in Colorado Springs. His informative talk to an audience of 90 technical professionals resulted in 18 new OPS Members. Please join us in welcoming those members on the Members Only Portal in the near future. Also of note is that we have seven OCP candidates writing their papers and three others who have also applied for the coveted OCP designation. Larry Pugliese, BoD and our Revenue Chair is planning the OPS Socials for May in San Antonio. He could use some help so email him at: Merchandise@OPSECSOCIETY.ORG

ÆGIS journal

Addressing threats that affect your bottom line

Volume 11 Number 8, August 2008

From the case files of

LUBRINCO

<http://www.lubrinco.com/>

1-212-695-1759

and

<http://www.feeinc.com/>

1-480-838-1728

Intellectual property and critical information being stolen or at risk? Call us!

This month's features:

Special Announcements

1. Asset Location and Due Diligence — AML implementation issues
2. OPSEC, Economic Espionage, and Competitive Intelligence — Sharing the news in China
3. Executive Protection — Sights for concealed-carry guns
4. Technical Issues — Illness and guns
5. Real Stories from the Field — Presidential politics: More lies on all sides
6. Book and Product Reviews — Vopt 9.0
7. Subscription/Unsubscription/Copyright Information

LUBRINCO has been short-listed by the Asian Development Bank for development of an Anti-Money Laundering program in Pakistan

L Burke Files will be speaking at:

- Sept 15th - 17th The 13th Annual International East West Security Conference, Rome, Italy
- Oct 16th - 17th Detectando al Empleado Deshonesto, A Comprehensive Look at Occupational Fraud and Money Laundering, Mexico City, Mexico
- Oct 20th – 24th International Structures - Panama City, Panama **Richard Isaacs will be speaking at:**
- December 9th – 15th International East-West Security Conference & Exposition, Malta

1. Asset Location and Due Diligence — AML implementation issues Someone we know pointed out that we had been saddled with the rather onerous Sarbanes Oxley not because companies were bad at record keeping, but because companies had been engaging in fraud and theft. As is almost always the case the legislation that came out of this over-reacted: All Sarbanes Oxley really needed to say was that auditors could no longer act as corporate consultants. What we end up with is a vicious circle of theft and fraud on the part of corporate managers followed by onerous regulation that makes for an unpalatable business climate here, inducing companies to go offshore. In the past there were other options available to deal with these issues. As an example, at one point shareholders could intervene. However, Justice Powell effectively quashed this remedy, so that shareholders are no longer a concern for managers. Another possibility would be better monitoring of existing regulations. Some find it comforting to know that inspectors are making sure that food processors are being watched to make sure that the food we buy won't kill us, that airlines are being inspected to make sure that planes won't fall out of the sky because of improper maintenance, and that corporations are being audited to make sure that they are not engaging in theft and fraud. However, lobbyists have been extremely effective in cutting down inspectors in all government agencies, and it is a safe guess that if the SEC again tried to make substantive inspections, their budget would be slashed. Note that inspection is designed to induce compliance. Enforcement comes after the breach of trust and fidelity. Compliance –not engaging in theft and fraud –comes before. Further, while there no doubt that an increased budget for the SEC would result in increased compliance, does the increased vigilance translate in to increased opportunity for the economy, or a disincentive to use the US? If inspection induces compliance it is good. If it is merely punitive it is bad. If companies leave the US because of a hostile environment it is bad. If they leave because they feel they can more easily engage in theft and fraud in another jurisdiction it may well be good. This balance is something we keep in mind when implementing AML programs, particularly in developing nations. On the one hand, we want to be compliant. Often this is the only interest of the hiring agency, particularly in the US. On the other hand, we also wish to actually cut down and detect money laundering: This is, in theory, what AML is about. Money laundering is an event used to gather funds from crime to support both criminals and the reinvestment of those proceeds into additional activities that are antithetical to government and the needs of the general population. Failure to prevent money laundering is economic fertilizer for the enemies of state and the common good. On the third hand, we do not want to create an environment that is hostile to business, and hinder economic growth rather than help it. It can be an uncomfortable balance until the gatekeepers get the real importance of what they are to do. Trying to get all three of these elements in place is a challenge, particularly if the only desire is to meet some minimal level of compliance – activity over substance – and then go back to business as usual.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Sharing the news in China

As part of the Olympics, hotels providing Internet access are being required by the Chinese government to install software to capture everything you send and receive. While those who travel regularly to China always assume that everything they do or say is monitored, it is possible that those coming to China for the Olympics may not be aware of this. Many hotels will show a pop-up window warning users that their activity will be monitored. However, it is possible that not all hotels will do so. Therefore, if you are going to China for the Olympics, be aware that everything you say, do, write, and read will be being shared with others. For most tourists this is not much of an issue: Everything they do will be as tourists, and completely above board. However, for those of a more political bent, or those engaging in business activities or dealing with sensitive commercial information, it is prudent to watch your step.

3. Executive Protection — Sights for concealed-carry guns

As readers know, we do not own, keep, or carry guns for personal protection. On the other hand, we are occasionally forced to carry guns as part of our professional obligations, and therefore shoot every day. We tend to carry one of two handguns, depending on the circumstances. The first is a 9mm ASP and the second is a .45ACP Smith & Wesson 625-3. The ASP came with the famed Guttersnipe sights, which we felt to be inappropriate for most work. We had them replaced by more conventional sights which worked as well or better at close distances as the originals, and worked much better at greater distances. Because the ASP tends to shoot where we point it, and has much less perceived recoil than a conventional 9mm, we are less concerned with its sights for short distances, or in conditions of

darkness. However, because of personal bias we prefer .45 ACP to 9mm. Therefore, much as we admire the ASP, unless there is some legal or logistical constraint, given our choice we will always opt for the .45ACP S&W 623-3. The 625 came with standard red ramp S&W front sights. These are excellent sights for many purposes – we shot the Secret Service match with this configuration, in spite of the fact that it has a totally inappropriate 3” barrel, and did not score at the bottom of the heap. Nonetheless, in a carry pistol our interest is not in shooting at one of the great ranges of the world, but in shooting in the dark at a target which is somewhere between next to us and ten feet away. (For our training outline, go to <http://www.lubrinco.com/lgptsht.html>). For a number of reasons, we felt we needed to look at other alternatives in terms of sights for this gun. In this situation, our interest is in sights that will help us get off the first shot. We decided on a tritium front sight so we would have at least some vague idea where the front of the gun was in relation to the target. Why not get tritium rear sights as well? Because in this situation we need to know where the target is and where the front of the gun is. Rear sights simply don’t contribute much in this situation. Our choice was the XS Sight Systems Big Dot Tritium Express Set, shown here on a Smith & Wesson 686. The big dot is **really** big, and easily picked up when it is light enough to see. As it gets darker, the tritium capsule in the center of the sight becomes visible enough to be seen for that important first shot. What about the remaining shots? There will be so much fire flying from the barrels of the guns being fired that this will not be a significant issue. The sights we got, the SW-0004S-3, retail for a modest \$90, and are well worth it. XS sights are among the best in the world, and if you carry a gun for work you should be speaking with them. If not, we believe you are doing yourself a disservice. XS Sight Systems (<http://www.xssights.com/>) are at 2401 Ludelle Street, Fort Worth TX 76105. Their phone number is 1-817-536-0136.

4. Technical Issues — Illness and guns

Recently this editor became (and still is) seriously ill. The good news was that any illness whose symptoms in any manner suggest a Viral Hemorrhagic Fever tends not to be ignored. The better news was that we got sick in Manhattan: The last time we were this sick was when we got cholera in Iran, an equally-amusing story which had some additional issues not relevant here. We learned a lot about being sick. If you call someone who is mostly sleeping, keep the call to a few minutes. If you go to visit, once it is clear that your presence has been recognized you can pretty much leave if the person is dozing. If you decide to show up with food, which will doubtless be appreciated, leave it and go. Don’t send text messages at 7am saying “I hope I’m not awakening you, but I just wanted to know how you are.” Don’t call at 1am. Call between 10am and 8pm. Shortly after getting sick we got a call from one of our be-armed-at-all-times friends suggesting that since we were in a vulnerable state, we really should have a loaded handgun on our nightstand. Putting aside the minor issue of our not having guns and ammunition at hand, this seemed pretty much crazy to us. Here we were, physically (we lost about ten percent of our body weight in two weeks), emotionally (we thought we were dying), and psychologically (when your temperature sails past 103 don’t count on really clear thinking, or on having a Piagetian level much above that of a six year old) at our worst, and someone wants us to keep a gun at hand? We instead chose an alternative to keeping a gun at hand: We simply spent two weeks sleeping, comforted by the fair assumption that since nothing bad had happened in the last 65 years, nothing bad would happen now. But what if something were to have happened? As an example, at one in the morning we got a call from our doorman saying the food we had ordered had arrived. Since we had not been able to eat for several days, we told him to have the delivery guy check the address, and went back to sleep. But what if the delivery guy were to have become psychotic, slipped by the doorman, and tried to beat our door down? Putting aside the minor issue that our door was unlocked so that neighbors caring for us could get in more easily, we had two approaches that seemed more reasonable than killing the delivery guy, and still allowed sleeping. The first would be to ignore the pounding and just stay in bed. The second would be to call 911, which would have produced a street full of police cars in under 30 seconds. However, neither of these was necessary. The doorman and the delivery guy figured out who had ordered the food, and we got to go back to sleep. Now it is certainly true that if you need a gun, there will be no adequate alternative weapon. That said, the odds of needing one while asleep in Manhattan are so slim as to not be worth considering. Often, however, you are in a situation where you don’t need a gun. As an example, another editor was once staying at his older sister’s for care while seriously ill. During the night a stalker broke into the home and was found rummaging through her clothes in her closet. Within a few seconds of reaching the intruder in the closet our intrepid editor violently vomited on the intruder, who screamed and left. The sister was thankful for the assistance, but not the carpet and dry cleaning bill. Keep your stomach loaded...

5. Real Stories from the Field — Presidential politics: More lies on all sides

As the political fight for the Presidency of the United States heats up, the lies have continued to flow in. Our recent favorite said, in essence, that while families of the 911 homicide victims, for reasons that have never been made clear us, got on average \$2 million each for having a relative be in the wrong place at the wrong time (the airlines got a rant of \$5 billion and \$10 billion in loans and the other roughly 6,500 Americans who died that day got nothing), the families of soldiers killed in action get 8 ducats and a wheel of cheese. OK, they actually had some dollar figures broken out, but it wasn't much more than that. We love cheese as much as the next person, but the figures listed didn't make much sense, so we went on line to check them, and they were wrong! In fact, it is a safe assumption that any startling revelation that supports or degrades a candidate is probably a lie. In the world of politicking, the current situation is very difficult. In most elections it is one candidate against another, or one position against another. You would think the latter would be the case, as there are a number of critical long term planning issues that need to be discussed, but are not being discussed. For example, neither candidate has said, "We have 300 million people in the United States. What do we want them to be doing for employment this year? In five years? In ten years? In 25 years?" Similarly, there is no discussion of long term energy policy (and no, "drill" or "don't drill" is not long term policy). Nobody has said (we are not policy makers, so what we are writing here is merely a sample of the *kind* of debate that we should, but are not, hearing), "In 30 years we want to be using hydrogen fuel for cars. To get there we will invest \$xxx. In the interim we want to move to electric cars and natural gas cars as a transition phase. Until that happens we will incentivize efficient current-technology and hybrid cars by giving a tax credit if your car gets over 50 miles a gallon highway, and a tax penalty if it gets under 20 miles per gallon highway. SUVs are *not* trucks, and will be penalized appropriately." "In addition, we need to decrease use of fuel by airplanes and trucks by finally implementing a maglev (<http://ntl.bts.gov/DOCS/TNM.html>) system. While trains are more efficient at carrying heavy loads than trucks, trucks are more efficient at carrying light loads. Since maglev is friction free, trucks will be able to carry light goods relatively short distances to a depot, with the maglev carrying the freight more efficiently for the long hauls. This will cut down on the overall use of trucks." "In addition, since maglev trains travel between 300 and 500 miles per hour, a lot of short haul airline travel will be eliminated. In theory you could stroll into Penn Station in New York at 8am and (if it were a direct train with no stops, which we admit is unlikely) get off the train at Union Station in Los Angeles at 3pm the same day. A well implemented maglev system could substantially cut down domestic air travel, and its associated fuel usage. If a closed-tube system were implemented the time to LA would be about three hours, which is rather astonishing. In the case of the Baltimore-Washington system (<http://www.bwmaglev.com/>), the time between the two cities will be roughly twenty minutes." "In addition, we want to cut down on oil-to-electricity conversion by moving to wind generated power where appropriate, hydroelectric power where appropriate, geothermal power where available, and solar power where reasonable, which should be enough to supply all of America's power needs with no oil usage. Short term we want to encourage municipalities to build and own their own power generation facilities, because the cost of electricity to citizens of the municipality will be lower – typically by a third – than buying from the grid (and we have read that one big wind turbine will provide electricity for 1000 homes). We also want to encourage more efficiently insulated houses so less power is needed for heating and cooling." While this is only a sample of the kind of debate over long term planning that we *should* be hearing, neither candidate is actually discussing *any* long term planning issues in *any* area. Instead, in this election what we have is not a discussion of issues, but John McCain running against the concept of change, with change being a rather amorphous quality. This leaves McCain with four obvious constituencies:

- Those who will not vote for a black man will vote for McCain.
- Those who believe that the primary function of the human race is to produce souls for God through Jesus, and that abortion, which deprives God of a soul, is a mortal sin will vote for McCain.
- Those who feel that the war in Iraq was appropriate and justified will vote for McCain.
- Those who believe the function of government is to ease the way for business and step back letting the economic benefits trickle down, and who believe *either* that our current economic malaise is caused by business-interfering big-spending Democratic social programs, *or* that the economy is thriving because of Republican policies, will vote for McCain. Obama, on the other hand, has only one ill-defined constituency: Those who want change, which they likely are unable to define with any clarity. The interesting factor here is that one might expect that this desire for

change might be enough to motivate the bottom forty percent of households – that is nearly half of all households – that share 0.2 percent (two tenths of one percent) of the country’s wealth to vote. As it turns out, this group is traditionally afraid of change because it almost always be for the worse, and they have no cushion from the bottom. In addition, in an election such as this the winner is likely to be the one that is most skilled in controlling either votes or voters. In the past, Democrats were the masters of voter fraud, but with the introduction of Direct Recording Electronic voting machines (DREs), the advantage has shifted to the Republicans. From a Republican perspective, therefore, one way to control votes is to get more states to use DREs: If you could get New York to go for DREs, Manhattan would vote Republican! Another way is to control voters is to use voter registration fraud to get rid of *undesirable* voters. According to Greg Palast, in swing-state Colorado the Republican Secretary of State conducted the biggest purge of voters in history, dumping twenty percent of all registrations, largely people of color. In swing-state Florida, the state is refusing to accept about 85,000 new overwhelming-black registrations from voter drives. In swing state New Mexico, half of the Democrats of Mora, a dirt-poor and overwhelmingly Hispanic county, found their registrations disappeared this year, courtesy of a Republican voting contractor. In swing states Ohio and Nevada, new federal law is knocking out tens of thousands of voters who lost their homes to foreclosure (no poll tax, no poll). This level of voter registration fraud – essentially uncontested by the Democrats – may already be enough to control the election. While potentially controlling the outcome of the election is good, from a PR perspective you don’t want tampering with votes or with voter registration to become an issue. In this case, it is not unreasonable to make up some preposterous scenario that suits your view of the world: Barack Obama eats children. Then pepper it with some bits of truth (Obama has said he loves children, and he and Michelle apparently both enjoy cooking), and send it forth. No matter how outlandish the story is, you will find some someone who will believe it. If you are lucky, you will also find some idiot who was sitting on the fence and for whom this will be the last bit of evidence – Do you want a President who eats children? – needed to gain their vote. How do these lies actually help the campaign? If voter or voter registration tampering is brought up, the appropriate response becomes, “You are getting caught up in paperwork issues and missing the real question: Do you want as President someone who eats children?”

6. Book and Product Reviews

Vopt 9

Golden Bow \$40.00

<http://www.goldenbow.com/> 1-619-298-9349

There are two easy ways to maximize the power of your computer. The first is to have as much memory as possible, and the second is to have your hard drive as defragmented as thoroughly possible. In this article, we will deal with the issue of defragmentation for the home user. While there are different sets of tools available for servers, for the home users we believe the best choice is Golden Bow’s Vopt, now in its ninth incarnation. We started using Vopt in the ‘80s, probably with version one, and suspect we have the original installation disk tucked away in a box somewhere in our storage space. Vopt has gotten faster and better over the years, and now includes a host of features which generally don’t concern us. What does concern us is Vopt’s ability to defragment a hard drive really quickly. This it does. If you wish to maximize the speed of your home computer, we strongly urge you to look at Vopt.

7. Subscription/Unsubscription/Copyright Information

•• AEGIS is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2008 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Philips (TPhillips@aegisjournal.com). LUBRINCO provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

Identification, valuation, and protection of intellectual assets and critical information.

American businesses lose \$300 billion in revenues annually to competitive intelligence, economic espionage, inappropriate disclosure, and information theft.

- LUBRINCO provides private sector consulting access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information.
- Implementing an OPSEC program is likely to increase revenues for an at-risk operating group by \$75 million.

International asset location and due diligence.

- Location of concealed assets in fraud, theft, and divorce.
- Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, and the Caribbean.
- Financial fraud, anti-money laundering, and anti-corruption program development and training.

□ **Protection of management, staff, and families.**

- In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
- When traveling and living overseas.
- When transporting items of substantial value. LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff. For information on LUBRINCO and its services, or for the archive of all past issues of *ÆGIS* in PDF format, please go to <http://www.aegisjournal.com/>. Subscription to *ÆGIS* is available for \$15 per year in North America and \$20 per year outside of North America. To sign up for a complimentary subscription to *ÆGIS* or the *ÆGIS* PDF notification list, send an email to subscribe@aegisjournal.com. To subscribe to our AvantGo channel, go to http://avantgo.com/channels/add_channel.pl?cha_id=1773 To be removed from the subscription list, send an e-mail to unsubscribe@aegisjournal.com. If you know of anyone else who should be receiving *ÆGIS*, please send their e-mail address to subscribe@aegisjournal.com. If there is a topic that you would like to know more about, send it to editor@aegisjournal.com and the editors will consider it as the topic for an article in an upcoming issue. If you would like to submit an article for publication in *ÆGIS*, send it as an attachment to an e-mail to editor@aegisjournal.com. Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in *ÆGIS* constitutes a license to LUBRINCO, and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose. If you would like to go beyond normal fair-use in reproducing articles from this issue of *ÆGIS*, you may do so freely as long as appropriate source, copyright, accreditation, and link to the *ÆGIS* Web site is included. This should be in the form *Article Title*, from the August 2008 *ÆGIS* (© 2008 LUBRINCO and FE&E), to be found at <http://www.aegisjournal.com/>. *ÆGIS* is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in *ÆGIS* should be construed as legal advice. The information provided is "general information," not "specific advice." The solution to any problem is highly dependent upon the precise facts involved. Thus, before making any reliance upon anything said here, you should consult with an appropriately skilled professional. Opinions expressed by contributors are not necessarily endorsed by the publisher, and may be presented to encourage a dialogue among subscribers. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in *ÆGIS*. Please be safe, and be smart.

National Security Institute
September 16, 2008

Security Awareness Solutions from NSI

The Employee Security Connection
is a quarterly security awareness newsletter for defense contractor and government employees.



In this issue

- FBI Wrestling With Remake as Intelligence Agency
- U.S. govt. focuses on securing backdoors in tech products
- Ex-Boeing worker admits sabotage
- One of 11 alleged T.J. Maxx hackers pleads guilty
- How does the CIA keep its IT staff honest?
- U.S. scans incoming air cargo
- House adopts overclassification reduction act
- In Hunt for Bin Laden, a New Approach
- WMD Report: US Remains Vulnerable
- New Metrics Assign Grades to Your Security Posture
- Spy agencies prepare for administration change
- Roles, Methods of Security Are Changing in Business
- Prosecutors: Woman had notes on NY sites, attack

FBI Wrestling With Remake as Intelligence Agency (WSJ, 9/16/08)

Seven years after the 2001 terrorist attacks, the Federal Bureau of Investigation is still facing challenges in remaking itself into a domestic-intelligence organization. Among the weak points found by an internal study: an insufficient number and quality of intelligence sources; a lack of understanding of what information should be collected; intelligence officers with limited awareness of their local areas; and quality-control problems with analysis.

FBI officials said they are implementing fixes to address the problems. According to documents reviewed by The Wall Street Journal, the study was performed last year to diagnose weaknesses they should address as they launched the FBI's latest initiative to improve intelligence collection and analysis, dubbed the Strategic Execution Team.

Several current and former intelligence and law-enforcement officials say the latest efforts still fall short of what is needed. In particular, they say, the FBI hasn't sufficiently addressed its gun-and-badge culture, which gives intelligence analysts a lesser status within the organization. [More](#)

U.S. government focuses on securing backdoors in tech products (Infoworld, 9/15/08)

As part of a comprehensive cybersecurity push, the U.S. government will focus on improving its network defense capabilities and on revamping acquisition rules to protect against malicious code installed during the manufacturing process of electronic devices. The National Cybersecurity Initiative, announced by President George Bush in January, will replace the government's outdated network perimeter defense system, officials from the U.S. Department of Homeland Security (DHS) and other agencies said at a Monday cybersecurity conference hosted by the Information Technology Association of America.

Officials from DHS, the White House and the Office of the Director of National Intelligence (DNI) used the conference to unveil new details about the cybersecurity initiative, which involves multiple government agencies. Government officials are increasingly concerned about hidden vulnerabilities and Trojan horses in commercial technology products, said Paul Schneider, deputy secretary at DHS. The U.S. government needs to better protect its supply chain, particularly when a growing number of tech products are produced overseas, he said. [More](#)

Ex-Boeing worker admits sabotage (AP, 9/12/08)

A disgruntled ex-Boeing worker admitted that he disabled a nearly finished, \$24 million military helicopter during his last shift on the assembly line. Matthew Montgomery, 33, of Trevoze, had applied for several transfers to other Boeing facilities, but was instead being moved to another job within the Ridley Park, Delaware County, plant. He used his work-issued wire cutters to sever about 70 electrical wires running together from the cockpit to the main body of an H-47 Chinook on May 10.

Montgomery pleaded guilty to one count of destroying property under contract to the government. Boeing officials focused on Montgomery within a week, and he readily admitted his role in a May 19 interview. The day Boeing officials found the severed wires, they also found a suspicious washer in the transmission of another Chinook at the plant. [More](#)

One of 11 alleged T.J. Maxx hackers pleads guilty (CNET News, 9/12/08)

One of the hackers accused of involvement in the massive data breach targeted at T.J. Maxx's parent company, arguably the largest security breach worldwide, reportedly pleaded guilty on Thursday. Damon Patrick Toey pleaded guilty to wire fraud, credit card fraud, and aggravated identity theft, and will be released subject to electronic monitoring, according to a report on the Wall Street Journal's Web site. Eleven defendants total are facing charges in federal court in Boston.

TJX Companies, the parent company of T.J. Maxx and Marshall's, said in March 2007 that 45.7 million accounts were compromised over nearly a two-year period. The company said--and federal investigators subsequently confirmed--that it believed the hackers gained access to millions of credit card and debit card numbers through inadequately protected Wi-Fi networks,

and then put the numbers up for sale. [More](#)

How does the CIA keep its IT staff honest? (Computerworld, 9/12/08)

Be prepared to go through a lot of scrutiny if you want to work in the Central Intelligence Agency's IT department, says chief information officer Al Tarasiuk. And it doesn't stop after you get your top secret clearance. "Once you're in, there are frequent reinvestigations, but it's just part of process here," says Tarasiuk, who also gets polygraphed regularly, though he won't be more specific. For those senior IT managers who are the "privileged users," meaning system administrators, "there is certainly more scrutiny on you," Tarasiuk says. "

There's so much top secret information contained within the CIA's systems that IT plays a key infosecurity role in making sure that CIA employees are not doing anything nefarious. There's also the persistent threat of foreign government intelligence agencies trying to break into the CIA's networks and databases. [More](#)

U.S. scans incoming air cargo (USA Today, 9/11/08)

The Homeland Security Department will put all incoming air cargo through radiation detectors at the nation's airports to try to prevent terrorists from smuggling radioactive bombs into the U.S. The new initiative aims to close what the 9/11 Commission's final report called a major security vulnerability — cargo on airplanes as a potential avenue for terrorism. Any cargo shipped on passenger planes will also be scanned.

Detectors have begun checking packages at Dulles International Airport outside Washington, D.C. Arriving cargo — whether from Pakistan or Peoria — will be driven through giant detectors called Radiation Portal Monitors. Although every piece of cargo will be scanned, "our focus is on the international cargo," says Jayson Ahern of Homeland Security's Customs and Border Protection division. [More](#)

House adopts overclassification reduction act (Secrecy News, 9/10/08)

The House of Representatives has passed the Overclassification Reduction Act, a bill that is intended to help reduce inappropriate classification of information in government.

The bill would require the National Archivist to develop regulations to help combat overclassification. The bill would mandate increased accountability for classification actions, with incentives for challenging improper classification and penalties for abuse of classification authority. Importantly, it would require agency inspectors general to perform periodic audits of classification activity to ensure compliance with classification standards. [More](#)

In Hunt for Bin Laden, a New Approach (Wash. Post, 9/10/08)

Frustrated by repeated dead ends in the search for Osama bin Laden, U.S. and Pakistani officials said they are questioning long-held assumptions about their strategy and are shifting tactics to intensify the use of the unmanned but lethal Predator drone spy plane in the mountains of western Pakistan. The number of Hellfire missile attacks by Predators in Pakistan has more than tripled, with 11 strikes reported by Pakistani officials this year, compared with three in 2007.

The attacks are part of a renewed effort to cripple al-Qaeda's central command that began early last year and has picked up speed as President Bush's term in office winds down, according to U.S. and Pakistani officials involved in the operations. There has been no confirmed trace of bin Laden since he narrowly escaped from the CIA and the U.S. military after the battle near Tora Bora, Afghanistan, in December 2001, according to U.S., Pakistani and European officials. They said they are now concentrating on a short list of other al-Qaeda leaders who have been sighted more recently, in hopes that their footprints could lead to bin Laden. [More](#)

WMD Report: US Remains Vulnerable (AP, 9/9/08)

The United States remains "dangerously vulnerable" to chemical, biological and nuclear attacks seven years after 9/11, a forthcoming independent study concludes. And a House Democrats' report says the Bush administration has missed one opportunity after another to improve the nation's security. The recent political rupture between Russia and the U.S. only makes matters worse, said Lee Hamilton, the former Indiana Democratic congressman who helped lead the 9/11 Commission and now chairs the independent group's latest study.

Efforts to reduce access to nuclear technology and bomb-making materials have slowed, thousands of U.S. chemical plants remain unprotected, and the U.S. government continues to oppose strengthening an international treaty to prevent bioterrorism, according to the report produced by the bipartisan Partnership for a Secure America. [More](#)

New Metrics Assign Grades to Your Security Posture (Dark Reading, 9/8/08)

A coalition of enterprises, government agencies, universities, and vendors from around the globe has released a set of free metrics for measuring an organization's security posture. The nonprofit Center for Internet Security (CIS) hopes the metrics will serve as a standard method for assessing security readiness. "Today there are thousands of ways to measure this... but no two organizations measure these things the same way, and no two divisions [in the same organization] measure them in the same way," says Bert Miuccio, CEO of CIS. "Today we are creating an objective, data-driven way to measure the security status of an enterprise."

Miuccio says this "number grade" can be used to help a company make more informed security buying decisions or change its security strategy, for instance. "This lets decision-makers understand the security status of their organization over time," he says. [More](#)

Spy agencies prepare for administration change (FCW.com, 9/5/08)

The intelligence community has begun to offer briefings to the two leading presidential candidates as the spy agencies prepare for the first presidential transition since a sweeping reform law passed in 2004. The law, which demanded greater integration of the nation's 16 intelligence agencies, reorganized the nation's intelligence community significantly, institutionally and technologically. It was largely a response to the criticism that U.S. intelligence efforts had incurred for not preventing the 2001 terrorist attacks and for faulty intelligence used to justify the Iraq War.

Sen. Susan Collins (R-Maine), who sponsored the 2004 intelligence reform law, said it represented a sea change in the structure and operation of the intelligence community. "Now the trail of dots terrorists leave behind as they plan, train and organize will never again be left unconnected," she said. The next president will inherit the new structure, which includes the Office of the Director of National Intelligence (ODNI) as the head of that community, and a workforce that has gotten younger and larger since 2001. [More](#)

Roles, Methods of Security Are Changing in Business (Dark Reading, 9/4/08)

The goals haven't changed. But for many security departments, the methods of getting there are gradually shifting on a tectonic level, a Forrester Research's security expert said. In his keynote address, Khalid Kark, principal analyst for security at the industry research firm, revealed data from Forrester's annual security survey which indicate that the ends of today's enterprise security efforts aren't changing, but the means are. "The good news is that ... security is becoming more visible in the organization," Kark said. "The bad news is that the security organization doesn't know how to deal with the visibility, and the problems are not well defined."

In a study of more than 1,100 security decision-makers at North American companies, Forrester found that after a slight dip in 2007, security is once again the top priority among IT departments, gaining the top spot in 50 percent of responding organizations. In fact, respondents said that when the year is through, security will make up 10 percent of IT spending, up from 8 percent a year ago. More than 20 percent of respondents expect security spending to increase in 2009.

[More](#)

Prosecutors: Woman had notes on NY sites, attack (AP, 9/2/08)

A U.S.-educated Pakistani woman was carrying handwritten notes referring to a "mass casualty attack" and listing the Empire State Building and other New York landmarks when she was detained in Afghanistan, prosecutors said. In an attempted-murder indictment unsealed in federal court in Manhattan, prosecutors for the first time publicly named some of the landmarks. The others: the Statue of Liberty, Wall Street, the Brooklyn Bridge and Plum Island, a disease research complex in Long Island Sound.

Aafia Siddiqui had notes "that referred to a 'mass casualty attack'" and to "the construction of dirty bombs, chemical and biological weapons and other explosives," the indictment said. "These notes also discussed the mortality rates associated with certain of these weapons and explosives." Other documents "referred to specific 'cells' and 'attacks' by certain 'cells' ... and

discussed recruitment and training," the papers said.

[More](#)

Keep Getting This Newsletter

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

TO SUBSCRIBE: If you were sent this by a colleague and wish to subscribe to NSI's complementary Security NewsWatch e-newsletter, visit <http://nsi.org/newswatch.html>.

TO UNSUBSCRIBE: This news service comes to you from the news team at the National Security Institute. 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 <http://nsi.org/newswatch.html>

Advertisers: For information about sponsoring this e-letter, contact sburns@nsi.org or call 508-533-9099.

National Security Institute

116 Main Street, Suite 200

Medway, MA 02053

Tel: 508-533-9099

Fax: 508-533-3761

Internet: <http://nsi.org>