(U) FBI Tampa Division
CI Strategic Partnership Newsletter
JANUARY 2012

(U) Administrative Note: This product reflects the views of the FBI-Tampa Division and has not been vetted by FBI Headquarters.

(U) Handling notice: Although UNCLASSIFIED, this information is property of the FBI and may be distributed only to members of organizations receiving this bulletin, or to cleared defense contractors. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

10 JAN 2012

(U) The FBI Tampa Division Counterintelligence Strategic Partnership Newsletter provides a summary of previously reported US government press releases, publications, and news articles from wire services and news organizations relating to counterintelligence, cyber and terrorism threats. The information in this bulletin represents the views and opinions of the cited sources for each article, and the analyst comment is intended only to highlight items of interest to organizations in Florida. This bulletin is provided solely to inform our Domain partners of news items of interest, and does not represent FBI information.

In the JANUARY 2012 Issue:

(U) NATIONAL SECURITY THREAT NEWS FROM GOVERNMENT AGENCIES:

(U) American Jihadist Terrorism: Combating a Complex Threat (*15 NOV 2011, Congressional Research Service*)

(U) In November, the Congressional Research Service released a report that describes homegrown violent jihadists and the plots and attacks that have occurred since 9/11. It discusses the radicalization process and the forces driving violent extremist activity. It analyzes post-9/11 domestic jihadist terrorist activity and describes law enforcement and intelligence efforts to combat terrorism and the challenges associated with those efforts. It also outlines actions underway to build trust and partnership between community groups and government agencies and the tensions that may occur between law enforcement and engagement activities. The report does not address terrorist activity against the United States conducted by foreigners, such as the airline bombing attempts by Farouk Abdulmutallab (Christmas Day 2009), the perpetrators of the Transatlantic Airliners plot (August 2006), or the "shoe bomber" Richard Reid (December 2001). Nor does the report address domestic terrorism attributed to violent extremists inspired by right-wing or left-wing ideologies and environmental, animal rights, or anti-abortion causes.

(U) According to a CRS press release: The report describes homegrown violent jihadists and the plots and attacks that have occurred since 9/11. 'Homegrown' and 'domestic' are terms that describe terrorist activity or plots perpetrated within the United States or abroad by American citizens, legal permanent residents, or visitors radicalized largely within the United States. The term 'jihadist' describes radicalized individuals using Islam as an ideological and/or religious justification for their belief in the establishment of a global caliphate, or jurisdiction governed by a Muslim civil and religious leader known as a caliph. The term 'violent jihadist' characterizes jihadists who have made the jump to illegally supporting, plotting, or directly engaging in violent terrorist activity. The report also discusses the radicalization process and the forces driving violent extremist activity. It analyzes post-9/11 domestic jihadist terrorism and describes law enforcement and intelligence efforts to combat terrorism and the challenges associated with those efforts. It also outlines actions underway to build trust and partnership between community groups and

government agencies and the tensions that may occur between law enforcement and engagement activities. One appendix provides details about each of the post-9/11 homegrown jihadist terrorist plots and attacks. A second appendix describes engagement and partnership activities by federal agencies with Muslim-American communities. Finally, the report offers policy considerations for Congress. There is an 'executive summary' at the beginning that summarizes the report's findings, observations, and policy considerations for Congress."

(U) Specific plots and attacks are described throughout the report to support analytic findings. A full description of each of the post-9/11 cases is provided in Appendix A of the report. The report also offers policy considerations for Congress. The Congressional Research Service is an arm of the Library of Congress that conduct research on topics of interest to the US Congress.

(U) Analyst Comment: This is a Congressional Research Service 145-page report - I highly recommend anyone interested in or working in counterterrorism, force protection or corporate security download and read this report. A full copy of the report can be downloaded at: www.fas.org/sgp/crs/terror/R41416.pdf

(U) Authorities Uncover Increasing Number of United States-Based Terror Plots (*The Pittsburgh Tribune-Review, 03 DEC 2011*)

(U) Authorities uncovered more United States-based terrorist plots in the past two years than they did in more than seven years following the Sept. 11 terrorist attacks, according to a research report submitted to Congress in November. Those busts included the January, 2011 arrest of an Armstrong County jihadist who provided advice and encouraged attacks on targets in the United States. Emerson Begolly, 22, of Redbank has pleaded guilty to and awaits sentencing on charges of soliciting terrorist acts and carrying a firearm in the commission of a violent crime.

(U)A La Roche College professor and retired FBI agent who studies terrorism, said the numbers don't reveal whether there is an increase in jihadist activity inside the United States, better detection of those activities or some combination. Local, state and federal law enforcement agencies are better able to detect people planning or advocating terrorist acts, and the public has become more aware of and is willing to report suspicious activity, so that could explain part of the increase, said the professor. Beyond that, "it's really hard to say that there's an increase in individuals who are willing to take violent action," he said.

(U) The Nov. 15 report by the Congressional Research Service looks only at plots developed by US citizens or permanent residents. The plots include those with targets inside the country as well as attempts by individuals and small groups to link up with international terrorist groups. Homeland Security committees from the House and Senate conducted a joint Dec. 7 hearing to examine the domestic terror threat to military communities.

(U) Of the 53 plots detailed in the report, 32 were discovered in the last two years, compared to 21 in the seven years following 9/11. Several plots targeted military facilities here and overseas as well as recruiting centers, including the Fort Hood, Texas, shootings, the Little Rock recruiting center shootings and the plot to attack soldiers at Fort Dix, New Jersey. Twenty-seven of the 53 acts were committed by "lone wolf" jihadists like Begolly, 19 of which were uncovered since 2009.

(U) The director of Penn State University's International Center for the Study of Terrorism said the Internet has made it easier for individuals to explore and adopt causes. "The thing about lone wolves is that they tend to be almost impossible to detect, but they're easy to catch," he said. "They also tend to be ineffective." Most individuals and groups detailed in the study fall into the category of "nihilist terrorists," the La Roche College professor said. These are people planning or committing violent acts or supporting others who do so, less out of a strong belief in their cause than in a desire to strike out at society, he said.

When asked to explain the cause for which they're supposedly fighting, "you find out that they're either lacking in knowledge completely or the knowledge base they have is delusional," he said. The Penn State Center director agreed that Islam plays a small role in many cases. A Minneapolis group arrested in 2009 for recruiting fighters from a Somali ethnic community to join a militant group in Somalia, for example, dwelt as much on the men's sense of duty to defend their homeland as it was on their Muslim beliefs. "We're finding that so many kinds of people are getting involved in homegrown terror that they really defy easy explanation," he said.

(U) Chinese Counterfeit COTS Create Chaos for the DoD (*RFGlobalnet, 22 NOV 2011*)

(U) On November 8, the Senate Armed Services Committee (SASC) held a hearing to explore the so-called "flood" of Chinese counterfeit electronic parts that have infiltrated the Department of Defense (DoD) supply chain since 2009. According to reports reviewed during the hearing, counterfeit electronic parts have been installed or delivered to the military for use in thermal weapons sights, on THAAD missile mission computers, and on military aircraft including the C-17, C-130J, C-27J, P-8A Poseidon, AH-64, SH-60B, and CH-46. The hearing focused on three cases where suspect counterfeit electronic parts were installed on military systems and subsystems manufactured by Raytheon, L-3, and Boeing.

(U) While investigations into the Chinese counterfeit parts are ongoing, what the preliminary SASC hearing uncovered is of great concern. Senators and defense industry leaders discussed the sources of counterfeit electronic parts and how they are made, as well as the cost and potential impact of counterfeit electronic parts on defense systems. The investigations also revealed that, in many instances, defense contractors were aware of the counterfeit parts but did not report them to the DoD in a timely manner.

(U) Evidence Leads To China

(U) During the hearing, committee members presented findings from several investigations into electronic part counterfeiting. One of these was a January 2010 Department of Commerce Bureau of Industry and Security report entitled "Defense Industrial Base Assessment: Counterfeit Electronics." The report was based on a survey of 387 companies and organizations in the DoD's supply chain, electronic parts manufacturers, distributors, assemblers, defense contractors, and the DoD itself. According to the report, the number of incidents of counterfeit parts increased from 3,868 in 2005 to 9,356 in 2008. The survey identified China as the source of counterfeit parts nearly 5 times more frequently than any other country.

(U) The Armed Services Committee launched its own investigation into counterfeit parts in the DoD supply chain in March 2011. Committee staff read more than 100,000 pages of documents identifying counterfeit parts, and also interviewed dozens of people from all segments of the DoD supply chain. The investigation revealed 1,800 cases of suspected counterfeit parts since 2009, which accounted for a million individual electronic parts. The committee then selected 100 of those cases to trace the origin of the parts. More than 70 percent of them were traced back to China, and many more were tracked to known resale locations for Chinese electronics in the United Kingdom and Canada.

(U) Many of the counterfeit electronic parts discovered in the DoD supply chain were salvaged from electronic waste shipped to Hong Kong from the United States and the rest of the world. The electronic waste ends up in counterfeiting districts of mainland China, such as Shantou in Guangdong Province, where electronic parts are burned off of old circuit boards, washed in a river, and dried on sidewalks. The parts are then sorted, and the original identifying marks are sanded off. Finally, the parts are recoated to hide the sanding marks, and state of the art equipment is used to print new counterfeit markings on the parts. The parts often look brand new after this process and are easily distributed around the world via the Internet.

(U) Raytheon's VP of Supply Chain Operations Vivek Kamath, who testified at the SASC hearing, said: "the amazing thing about [Chinese electronic counterfeiting] is it's very open. There is nothing discreet about it. And it's just almost as if it's just accepted as another business model in the country." So far, the Chinese government refuses to take action against counterfeiting industry.

(U) Threat to the United States

(U) Counterfeit electronic parts clearly threaten the performance and reliability of US defense systems, even if the parts pass acceptance tests. In the case of the US Navy SH-60B helicopter, for example, the counterfeit parts affect the forward looking infrared (FLIR) system, which provides night vision capability to the pilot and laser targeting for Hellfire missiles. If the FLIR system fails, the pilot's ability to identify targets and avoid hazards at night is compromised, and the SH-60B cannot conduct surface attacks using its Hellfire missiles. The reliability of the FLIR system puts the helicopter's availability in question and endangers the lives of soldiers that use the platform.

(U) The SASC also acknowledged a secondary issue: how the rampant theft of US intellectual property by Chinese counterfeiters severely impacts our economic security. According to the Semiconductor Industry Association (SIA), counterfeiting puts the current jobs of 200,000 American semiconductor workers at risk. SIA estimates that counterfeiting costs US semiconductor manufacturers $7.5 billion a year in lost revenue and costs workers nearly 11,000 US jobs.

(U) Opening Statement at SASC Hearing on Counterfeit Electronic Parts in DOD Supply Chain Tuesday, November 8, 2011

(U) This is an excerpt from the Opening Statement on Suspect Counterfeit Parts in the US Navy SH-60B Helicopter:

(U) I (Senator Levin) am now going to run through a presentation of how one of these counterfeit parts made its way through the defense supply chain. The SH-60B is a Navy helicopter that conducts anti-submarine and anti-surface warfare, surveillance and targeting support. The SH-60B deploys on Navy cruisers, destroyers, and frigates and has a Forward Looking Infrared or "FLIR" System which provides night vision capability. The FLIR also contains a laser used for targeting the SH-60B's hellfire missiles.

(U) On September 8, 2011, the Raytheon Company sent a letter to the US Naval Supply Systems Command alerting the Navy that electronic parts suspected to be counterfeit had been installed on three Electromagnetic Interference Filters (EIF) installed on FLIR units delivered by Raytheon. Raytheon only became aware of the suspect counterfeit after being alerted by the Committee's investigation. According to the Navy, the failure of an EIF could cause the FLIR to fail. The Navy also told the Committee that an SH-60B could not conduct surface warfare missions involving hellfire missiles without a reliable, functioning FLIR. A FLIR failure would also compromise the pilot's ability to avoid hazards and identify targets at night, limiting the SH-60Bs ability to be deployed in night missions. One of the FLIRs was sent to the USS Gridley in the Pacific Fleet.

(U) Senator Levin's full opening statement has additional examples and witness testimony. Click here to access the full Statement with exhibits:
http://levin.senate.gov/newsroom/speeches/speech/opening-statement-at-sasc-hearing-on-counterfeit-electronic-parts-in-dod-supply-chain

(U) DHS Releases Cyber Strategy Framework (*fiercegovernmentit.com, 14 DEC 2011*)

(U) The Department of Homeland Security released its cybersecurity strategy on December 12, 2011, calling it a "Blueprint for a Secure Cyber Future." The framework aims to help it better use existing capabilities and promote technological advances that make government, the private sector and the general public more resilient online, said DHS Secretary Janet Napolitano in a Dec. 12 blog post. **The strategy document focuses on two core areas of DHS's cyber mission: protecting critical information infrastructure and strengthening the broader cyber ecosystem.**

(U) According to the blueprint, DHS will protect critical information infrastructure by reducing exposure to cyber risk, ensuring priority response and recovery, maintaining shared situational awareness and increasing resilience. As part of that goal, DHS with its partners will design, deploy and operate the National Cybersecurity Protection System. It will also develop incident reporting guidelines, issue alerts regarding significant threats or incidents, and run the National Cybersecurity and Communications Integration Center, according to the plan. DHS will also maintain the National Cyber Incident Response Plan; lead, integrate and coordinate critical infrastructure protection; and lead enterprise wide efforts to secure systems across federal civilian agencies and departments.

(U) The other half of DHS responsibilities under the plan relate to four goals for strengthening the cyber ecosystem. The strategy says DHS aims to empower individuals and organizations to operate securely; make and use more trustworthy cyber protocols, products, services configurations and architectures; build collaborative communities; and establish transparent processes.

(U) Toward those goals DHS will take on a more active role with education, and research and development. Implementing the National Initiative for Cybersecurity Education will fall under DHS's purview, according to the plan. It will also work with the Defense Department and research agencies to develop cybersecurity capabilities. The blueprint says DHS will "align" its activities to the National Strategy for Trusted Identities in Cyberspace, "including further alignment with the Federal Identity, Credential and Access Management Roadmap." It will also fund and support the development and implementation of interoperable tools, architectures, policies and standards for use across government.

(U) The blueprint draws heavily from concepts presented in the White House's National Security Strategy and goals set in the 2010 Quadrennial Homeland Security Review. The QHSR highlighted safeguarding and securing cyberspace as a key mission of the department. **The full strategy can be downloaded at: http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf**

(U) COUNTERINTELLIGENCE/ECONOMIC ESPIONAGE THREAT ITEMS FROM THE PRESS

(U) United States Homes In on China Spying (*13 DEC 2011, The Wall Street Journal*)

(U) US intelligence agencies have pinpointed many of the Chinese groups responsible for cyberspying in the United States, and most are sponsored by the Chinese military, according to people who have been briefed on the investigation. Armed with this information, the United States has begun to lay the groundwork to confront China more directly about cyberspying. In early December, US officials met with Chinese counterparts and warned China about the diplomatic consequences of economic spying, according to one person familiar with the meeting.

(U) The Chinese cyberspying campaign stems largely from a dozen groups connected to China's People's Liberation Army and a half-dozen nonmilitary groups connected to organizations like universities, said those who were briefed on the investigation. Two other groups play a significant role, though investigators haven't determined whether they are connected to the military. In many cases, the National Security Agency has determined the identities of individuals working in these groups, which is a critical development that provides the United States the option of confronting the Chinese government more directly about the activity or responding with a counterattack, according to former officials briefed on the effort. "It's actually a small number of groups that do most of the PLA's dirty work," said a cybersecurity specialist at the Center for Strategic and International Studies (CSIS) who frequently advises the Obama administration. "NSA is pretty confident of their ability to attribute [cyberespionage] to this set of actors."

(U) In early November, the US chief of counterintelligence issued a report that was unusually blunt in accusing China of being the world's "most active and persistent" perpetrator of economic spying. Lawmakers have also become more vocal in calling out China for its widening campaign of cyberespionage. Still, diplomatic considerations may limit the United States interest in taking a more confrontational approach because some US officials are wary of angering China, the largest holder of US debt.

(U) Chinese Foreign Ministry spokesman Liu Weimin said that Chinese law "clearly prohibits hacking" and that the Chinese government "cracks down on such behavior and actively participates in international cooperation." "Accusations that China participates in such hacking, or that the Chinese government is behind it, are totally ungrounded," he said. Chinese officials regularly dispute US allegations of cyberspying, saying they are the victims, not the perpetrators, of cybercrime and cyberespionage. An NSA spokeswoman declined to comment.

(U) Identifying adversaries has been difficult because it is easy to fake identities and locations in cyberspace. An inability to tie cyberspying activities with precision to a certain actor has in the past limited the United State's ability to respond because it's hard to retaliate or confront an unidentified adversary. The US government, led by the National Security Agency, has tracked the growing Chinese cyberspying campaign against the United States for decades. More recently, NSA and other intelligence agencies have made significant advances in attributing cyberattacks to specific sources, mostly in China's People's Liberation Army, by combining cyberforensics with ongoing intelligence collection through electronic and human spying, the CSIS cybersecuity specialist said.

(U) The US investigation of China's activities is the latest round of spy-versus-spy in cyberspace. The activity breaks down into cyberspying efforts by 20 groups with different attack styles that are responsible for most of the cyber theft of US secrets, said the people briefed on the investigation. US intelligence officials have given different classified code names to each group. US intelligence officials can identify different groups based on a variety of indicators. Those characteristics include the type of cyber attack software they use, different Internet addresses they employ when stealing data, and how attacks are carried out against different targets. In addition to US government agencies, major targets of these groups include US defense contractors, according to former officials.

(U) Collectively, these groups employ hundreds of people, according to former officials briefed on the effort. That number is believed to be small compared to the estimated 30,000 to 40,000 censors the Chinese government is believed to employ to patrol the Internet. The Chinese government is believed to have been behind a number of recent major cyberbreak-ins, including multiple hacks of Google Inc. and the EMC Corp.'s RSA unit, which makes the numerical tokens used by millions of corporate employees to access their network. A cyberattack revealed this year on Lockheed Martin Corp. is also believed to have been traced to China, and the Chinese are believed to have been responsible for an infiltration a few years ago of the Pentagon's Joint Strike Fighter weapons program, which is also managed by Lockheed.

The counterintelligence report released last month predicted that China's espionage efforts will continue to grow.

(U) Opinion: China's Spies Are Catching Up (*The New York Times, 11 DEC 2011*)

(U) Note – This Opinion article by David Wise, author of the book "Tiger Trap, America's Secret Spy War with China" was published in the 11 DEC 2011 issue of the New York Times

(U) IN 1995, a middle-aged Chinese man walked into a CIA station in Southeast Asia and offered up a trove of secret Chinese documents. Among them was a file containing the top-secret design of the American W-88 nuclear warhead that sits atop the missiles carried by Trident submarines. He told a story to the CIA that was so bizarre it might just be true. He said that he worked in China's nuclear program and had access to the archive where classified documents were stored. He went there after hours one night, scooped up hundreds of documents and stuffed them into a duffel bag, which he then tossed out a second-story window to evade security guards. Unfortunately, the bag broke and the papers scattered.

(U) Outside, he collected the files and stuffed them back into the torn bag. Although many of the documents were of interest for their intelligence content, it was the one about the W-88 that roiled American counterintelligence most because it contained highly classified details about a cutting-edge warhead design. The United States had been producing small nuclear warheads for decades, and the Chinese were desperate to find out how to build miniaturized warheads themselves. China's military was, and still is, playing catch-up to the United States. China's success in obtaining the secret design of the W-88 is the most dramatic example of a fact that United States counterintelligence agencies have been slow to recognize: just as China has become a global economic power, it has developed a world-class espionage service — one that rivals the CIA.

(U) During the cold war, dozens of counterintelligence agents in the FBI and the CIA pursued Soviet and then Russian spies. The K.G.B. was seen as the enemy; China took a back seat. Only a handful of FBI special agents specialized in Chinese spy cases, and their work was not regarded as career-enhancing. Washington's ongoing failure to make Chinese espionage a priority has allowed China to score a number of successes in its espionage efforts against the United States.

(U) China's foreign intelligence service and its military intelligence agency actively spy on the American defense industry, our nuclear weapons labs, Silicon Valley, our intelligence agencies and other sensitive targets. In January, when Robert M. Gates, then the defense secretary, was visiting China, Beijing unveiled a stealth fighter jet, the J-20. The disclosure demonstrated that China had achieved a stealth capability, allowing it to conceal its planes, ships and missiles from radar — similar to the American stealth technology that China has been seeking to acquire by clandestine means for years.

(U) Later that month, an engineer who worked on the B-2 stealth bomber for Northrop Grumman was sentenced to 32 years in prison for passing defense secrets to China. In exchange for more than $100,000, he had helped design a stealth exhaust system for China's cruise missiles to make it difficult to detect and destroy them. And in August, reports attributed to American intelligence officials asserted that Pakistan had allowed Chinese experts to inspect the remains of the stealth helicopter that crashed during the May mission to kill Osama bin Laden. Although Pakistan and China denied the reports, Beijing would have a great interest in examining the tail of the Black Hawk helicopter, the part of the aircraft that was not destroyed by the Navy Seals team, to learn more secret details of American stealth technology.

(U) Meanwhile, the mystery of the leaked W-88 warhead design remains unsolved. At first, the American government suspected that Wen Ho Lee, a Los Alamos nuclear scientist, had leaked the W-88, but it produced no evidence that he had done so. He was held in solitary confinement for nine months, eventually pleaded guilty to one count of mishandling classified information and won an extraordinary apology from the federal judge who presided over the case. Misled by the Energy Department, the FBI had chased the wrong person for three years. Finally, in 1999, Robert Bryant, then the bureau's deputy director, enlisted Stephen Dillard, a veteran counterintelligence agent, to head a major investigation of how China had acquired the design of the W-88.

(U) The inquiry was led by the FBI and run by a task force of 300 investigators from 11 federal agencies, including the Defense Department, the CIA, the National Security Agency and the Defense Intelligence Agency. On Sept. 11, 2001, some of the investigators were killed when American Airlines Flight 77 was flown by terrorists into the Pentagon. But the investigation went on. Mr. Dillard's task force, operating out of public view, looked at the nuclear weapons laboratories, government agencies and defense contractors in California and several other states who had manufactured parts of the warhead. The FBI interviewed the walk-in, who was by now living in the United States, but he could shed no light on the source of the document. Finally, after four years, the investigation ended with American intelligence agencies no closer to knowing how China obtained the secret design of the nuclear warhead. The answer remains locked up in Beijing.

(U) More than a decade later, China's spies continue to conduct espionage against military targets. Last year, a Pentagon official was sentenced to prison, the last of 10 people rounded up by the F.B.I., all members of a loosely connected Chinese spy network on the West and East Coasts that was run by Lin Hong, a spymaster in Beijing. The data that made its way to China included information on the Navy's Quiet Electric Drive, designed to make submarines harder to detect, the B-1 bomber and projected American arms sales to Taiwan.

(U) China has even penetrated the FBI In 2003, Katrina Leung, an FBI informant for two decades, was found to be working as a double agent for Beijing. Astonishingly, the two top FBI agents in California responsible for Chinese counterintelligence were having affairs with Ms. Leung at the same time, allowing her to help herself to classified documents that were brought to her home by one of the agents. China's success in stealing American secrets will provide a continuing challenge to the spy catchers. And Washington's counterintelligence agents, accustomed to the comfortable parameters of the cold war and more recent battles against Al Qaeda, must rethink their priorities and shift their focus, resources and energy eastward to counter China's spies. If not, more secrets like the W-88 nuclear warhead will continue to find their way to Beijing.

(U) Canadian Politician's Chinese Crush Likely 'Sexpionage,' Former Spies Say (*The Toronto Star, 30 NOV 2011*)

(U) The Conservative government in Canada should have been more concerned when it was discovered one of its MPs was having a relationship with a reporter for China's state news agency, says a defector from the country's spy service. Li Fengzhi, a former agent with China's Ministry of State Security, says politicians like Foreign Affairs parliamentary secretary Bob Dechert are a top target of Chinese spies keen on learning about Canadian secrets, or grooming advocates for Beijing in Canada's corridors of power.

(U) Dechert's relationship with Toronto-based Xinhua reporter Shi Rong was revealed when someone hijacked her email account and forwarded a series of intimate messages she received from the Mississauga politician in the spring and summer of 2010. The leak was traced back to an apparent domestic dispute with Shi's husband. Li, who defected to the United States in 2003 and is now believed

to be working for the Central Intelligence Agency, was speaking to a high-level conference here on espionage through video link. For security reasons, his location was not disclosed. He said it is not possible to say with certainty that a Xinhua reporter is providing intelligence back to Beijing, but the act of striking up a relationship with an elected official fits the modus operandi of Chinese spies. "That's the normal way to get the job done," he said.

(U) Shi was called back to China when the relationship hit the news, which is another reason to be suspicious, Li said. "If the lady was called back to China very soon, I think it's possible she has some relationship with the security services, even if she's not an official agent of the Chinese security services," he said. "Other agents would try to get close to her . . . and use her as a bridge to get some intelligence from the politician or to influence the politician." Despite his declarations of "love" for the reporter, the married Dechert said that their relationship was merely "flirtatious."

(U) A follow-up investigation by the RCMP and the Canadian Security Intelligence Service found no evidence that national security had been compromised in the affair, CTV News reported in September. Nevertheless, the Canadian government should pay greater attention to such activities, Li said. A former CSIS agent agrees, saying the federal Conservatives have shown particularly poor judgment on security and intelligence matters involving its own officials over the years.

(U) The Dechert matter is but one example. There is also former foreign minister Maxime Bernier's relationship with a woman once linked to Quebec biker gangs, and former PMO adviser Bruce Carson's financial woes, multiple fraud convictions and relationship with a former escort. More recently, Arthur Porter was forced to resign as chair of the Security Intelligence Review Committee over his business ties to a former Israeli spy and international lobbyist who has done work for Zimbabwean dictator Robert Mugabe. "There's a great disconnect," said Michel Juneau-Katsuya, a former CSIS agent. "The problem that we have is that common sense doesn't prevail in the political leadership."

(U) Though intelligence officials have long warned of the threat from spies targeting politicians, Canadian industry is most at risk, he said. Prominent Canadian corporations like Bombardier and BlackBerry maker Research In Motion have already been targeted by Chinese firms intent on copying their successes. More recent interest in Canada's natural resources, such as the Alberta oil sands, from China is a growing threat.

(U) A CBC report this week on an investigation into a series of cyber attacks targeting federal government systems and several Toronto law firms traced it back to Chinese hackers looking for information on the proposed sale of Saskatchewan's Potash Corp. by Australia's BHP Billiton. "Canada is key for China because Canada has access to all the secrets of the big guys — G8, G20, NATO, NORAD. Name it and we have access to it," said Juneau-Katsuya. "Second, we have been friendly to them since the Trudeau era. They've been placing people in various levels of government for decades." He said that Dechert quite likely had no intention of betraying Canada in striking up a relationship with the young Chinese reporter, but he "got lured," said Juneau-Katsuya. "He got sort of distracted and they use that on a regular basis. This is a typical sexpionage situation."

(U) Analyst Comment: As this article highlights, the threat of Chinese espionage directed against sensitive proprietary corporate information may be greater than the threat of espionage against US government or military information. Florida companies doing business in China or in joint ventures with Chinese companies should be aware of these threats and conduct risk analysis on information sharing and network security.

(U) Foreign Hackers Targeted Canadian Firms (*CBC News, 30 NOV 2011*)

(U) A leading cyber-crime expert says foreign hackers who launched a massive attack on Canadian government computers last fall also broke into the data systems of prominent Bay Street law firms and other companies to get insider information on an attempted $38-billion corporate takeover. Daniel Tobok, whose international cyber-sleuthing company was called in by a number of the firms hit by the attacks, says the hacking spree from computers in China were all connected to last year's ultimately unsuccessful takeover bid for Potash Corporation of Saskatchewan."All those different attacks on companies, law firms and government were all interconnected, they weren't isolated incidents," he said in an interview with CBC News.

(U) The cyber-forensics guru with prominent clients around the world calls the assault on Canadian companies and the government "one of the biggest attacks we have ever seen." Tobok said hackers penetrated the computer systems of at least seven of Canada's leading law firms in what experts believe was an attempt to mask the real target of the attacks — the few firms directly involved in the aborted Potash deal. The foreign hack-attack on Canadian law firms was "very sophisticated and highly targeted," he said.

(U) The hackers appeared to have been hunting exclusively for information on the Potash deal, and there was no evidence they had penetrated the confidential files of other clients of the firms affected. "I think the law firms did a pretty good job in dealing with this attack … and no other clients were harmed. I mean this was not a fishing expedition to download all of the law firms' client files." One of the law firms representing PotashCorp in the deal is Bay Street's legendary Stikeman Elliott. In a prepared statement, the firm told CBC News it is "aware of the threat posed by hackers, as well as by viruses, malware and other means of infiltrating computer systems. "Accordingly, there are safeguards, audit processes and other measures in place that we believe to be appropriate. "We cannot comment on client matters specifically, but can say that we are not aware of any compromised client information as a result of our systems being breached."

(U) In a similar statement, another prominent law firm involved in the Potash deal, Blake, Cassels & Graydon, said it was "not aware of any compromise of client information as a result of any attempt to breach our systems." "We take our obligations of confidentiality to our clients and the integrity of our systems very seriously," the firm said.

(U) Tobok said, at first, no one investigating the Potash cyber-attacks connected the dots between the widespread attack on the government and similar invasions of the law firms and other companies. He said his company was first called in to investigate a series of odd computer glitches at one of the firms hit in the attacks. "We received a direct call just like we do every other day, (saying) 'I think that we have a problem here. Here is what is happening. Can you guys come and take a look at it?' "And nobody knew the severity of the issue or what was happening. They were just noticing that they had a problem."

(U) That was not long after the giant Australian resources conglomerate BHP Billiton had launched its ultimately unsuccessful bid for Potash Corp in August 2010, and several months before the federal government revealed its own computers had been hacked. Over the ensuing few months, Tobok's company got similar calls from at least two other firms, and that's when his investigators began to notice a pattern. "While there are hundreds of attacks a year, there were certain things about those attacks that had a certain signature on them that made it all connected," he said.

(U) Tobok says eventually investigators "at a very high level" were able to match that signature to the attacks on the federal government. The Conservative government finally stepped in and killed the whole Potash deal, but not before federal computer systems had taken the hardest cyber-hit of all. The hackers' successful penetration of the Canadian government computers forced federal security officials to shut down of all internet connections to the federal Finance Department and Treasury Board, along with Defense Research and Development Canada, an agency of the Department of National Defense, in an attempt to prevent the further theft of sensitive data. Almost a year later, all three departments are still without full internet access.

(U) The government initially tried to downplay the severity of the attack, claiming no information had been stolen. But a government memo obtained by CBC News earlier this year stated that "data has been exfiltrated and privileged accounts have been compromised." **The hackers used the same so-called "spear-phishing" technique to break into otherwise highly protected computers in the government, law firms and other companies hit by the attacks. The hackers sent each target organization a series of emails purporting to be from senior federal officials or firms involved in the PotashCorp deal. When infected email attachments were opened, they embedded in the target computer network so-called "malware" specifically designed to gather information on the PotashCorp deal.**

(U) Exactly why hackers went to such extraordinary lengths to get inside information on the ultimately ill-fated PotashCorp takeover remains a matter of some speculation. **China, one of the world's biggest consumers of potash-based fertilizers, was reportedly against the takeover bid that would have put the world's largest producer in the hands of BHP. The Financial Times reported that China's state-owned chemical company, Sinochem Group, had even hired several large international investment banking firms to assess ways to disrupt the BHP takeover bid.** The Chinese government has denied any role in the cyber-espionage fiasco, and experts say the fact the computers used in the attacks were in China does not necessarily mean the hackers were there, too.

(U) At the time of the attack, Russian interests were also rumored to be eying a possible takeover of PotashCorp if the BHP bid failed. While Tobok isn't pointing fingers, he estimates the PotashCorp attack had to have involved more than 100 hackers, leaving little doubt in his mind the whole thing was the work of a foreign intelligence service, or was otherwise "state-sponsored." He says the hacking methods used were so sophisticated the intruders almost completely erased their tracks after the attacks. Almost. "No crime is perfect," he said.

(U) Analyst Comment: As this article notes, cyber intrusions into unclassified corporate networks are often launched through “spearphishing” email attacks in which unsuspecting employees open email attachments that contain malware. Security managers and IT administrators should ensure that all employees receive training about spearphishing and most importantly, why it is such a critical threat to the network.

(U) Utah Scientist Charged With Stealing Drug Recipes (*Associated Press, 29 NOV 2011*)

(U) A scientist has been charged with stealing secret recipes from a Utah chemistry company and turning them over to his brother-in-law in India, in what federal authorities say is a crime rarely reported by US companies fearing they will be devalued. It's the first time authorities have filed industrial espionage charges in Utah, said a special agent with the FBI's Salt Lake City office.

(U) Prabhu Mohapatra, 42, worked for Frontier Scientific Inc., a North Logan company that supplies chemicals for research and drug discovery, said its chief executive. He said Frontier is the only company in the world that can make large, pure quantities of an organic chemical that has several applications,

from an ingredient in new drugs to solar cells and batteries. The chemical goes by the name 2,2'-dipyrromethane. "Our knowledge in making these chemicals is really our value," the Frontier CEO said. "It's a compound mostly unique to us. We developed the recipe for large quantities" that can be worth millions of dollars per kilogram.

(U) The federal complaint alleged that Mohapatra emailed the secrets to his in-law, who was setting up a unregistered, competing company in India called Medchemblox. Authorities tracked Mohapatra's moves on a company computer. The complaint quoted Mohapatra saying he had an interest in Medchemblox, and emails released by authorities showed Mohapatra trying to cover his tracks under fear of suspicion. "Please do not make any product currently present in Frontier Scientific's catalogue," Mohapatra wrote on Oct. 29 to his brother-in-law, according to the complaint. "I will lose my job and even could face jail time."

(U) The Frontier CEO declined to comment on the potential harm to his company. The federal complaint alleged that Medchemblox intended to undercut Frontier by becoming a supplier for the German chemical company Porphyrin Systems. The special agent said the FBI was investigating the "foreign nexus." Mohapatra pled not guilty at his Dec. 8 arraignment on a count of theft of trade secrets, his public defender said. He was arrested November 14 and released the same day after appearing in federal court in Salt Lake City. The FBI was holding his passport, according to a case that remained sealed until late Monday. He faces up to 10 years in prison and a $250,000 fine if convicted.

(U) The FBI Special agent said industrial espionage is a crime that often goes unnoticed "until you see a competitor showing up with a similar product." Federal authorities are trying to encourage US companies to report thefts of intellectual property, but many companies handle them internally, afraid the news will lower their company's stock value or send investors fleeing, he said. "In some cases, there's just a lack of awareness that the threat is out there," he said.

(U) Until 1996, the theft of trade secrets wasn't a federal crime, and the FBI had spotty success trying to prosecute such cases using various other statutes, such as wire fraud. Congress then passed the Economic Espionage Act, giving the FBI full authority to pursue the cases. **The Frontier CEO said he wasn't reluctant to report Mohapatra to authorities. “We're a small company and we don't have the stick like the US government," he said. "Quite often when these trade secrets are stolen, there isn't any recourse for a small company like ours. We didn't hesitate at all."**

(U) **Analyst Comment**: As the CEO of Frontier notes, it is important to report possible compromises or thefts of intellectual property to the FBI. Any company in Florida with this type of information should contact the FBI Tampa Strategic Outreach Coordinator, Patrick Laflin at 813-253-1029.

(U) Ohio Company and Three Individuals Indicted for Illegally Exporting Military Technology to South Korea (*US Department of Justice Press Release, 20 DEC 2011*)

(U) An indictment was returned in December by a federal grand jury sitting in Cleveland, Ohio, charging EO System Company, Ltd. and Seok Hwan Lee, Tae Young Kim and Won Seung Lee, with five counts of knowingly and willfully exporting, causing to be exported, and aiding and abetting the export of defense articles on the US Munitions List without first obtaining an export license or written authorization from the US Department of State, said Steven M. Dettelbach, United States Attorney for the Northern District of Ohio, and Stephen D. Anthony, Special Agent in Charge of the Cleveland Field Office, Federal Bureau of Investigation.

(U) EO System Company, Ltd. is, a corporation located in Inchon, Republic of Korea (South Korea), while Lee, Kim and Lee are citizens and residents of South Korea. "These defendants are charged with violating important regulations designed to protect national security," Dettelbach said. "The FBI and Department of Justice are committed to the protection of US defense technology, particularly that which is governed by the International Trafficking in Arms Regulations," Anthony said.

(U) The indictment charges that on or about November 4, 2005, the defendants knowingly exported, caused to be exported, and aided and abetted the export from the United States to the Republic of Korea (South Korea) of five (5) DRS PN: 42-15-050-003, E3500 system 25.7 mm F/1.0 Telescopes, also described as Infra Red Focal Plane Array detectors and Infra Red camera engines, which were designated as defense articles on the United States Munitions List. The indictment charges that the defendants did so without first obtaining an export license or written authorization for such export from the US Department of State.

(U) In a related case, Kue Sang Chun, 67, of Avon Lake, Ohio, previously pleaded guilty to one count of exporting defense articles on the US Munitions List without first obtaining an export license of written authorization from the State Department, and one count of knowingly making and subscribing a false US individual income tax return. He was sentenced to in November to 14 months in prison.

(U) Japan Firm Raided over Tech Exports to China (*AFP, 29 NOV 2011; Japan Economic Newswire, 29 NOV 2011*)

(U) Japanese police raided a Tokyo-based company in later November over allegations that it exported to China technical hardware that could have military applications, reports said. Police entered the headquarters and other offices of Intertec, which sells used electronic devices, including machines that produce semiconductors, according to footage broadcast by major television networks.

(U) Kanagawa prefectural police officials said Intertec Corp. allegedly exported about 500 sets of second-hand semiconductor manufacturing equipment with built-in automatic control programs to China around the spring of 2010 without obtaining permission from the trade minister. Police suspect semiconductors produced in China with the equipment might have been used to develop missile control devices.

(U) The foreign exchange and foreign trade law requires traders to obtain government permission when they export goods or technologies considered to possibly obstruct the maintenance of international peace and security. Founded in November 1994, Intertec deals in used semiconductor-production equipment and parts, and has branches and affiliated firms in Japan, Taiwan and Shanghai, China.

(U) CYBERSECURITY SPECIAL FOCUS FOR INDUSTRY:

(U) Best Ways To Detect Advanced Threats Once They Invade; Security Experts Offer Advice on How to Detect the Intrusion (*Dark Reading, 05 DEC 2011*)

(U) Significant attacks against major technology companies have underscored that, while good defenses can make it hard for an attacker to penetrate a network, a persistent attacker will find a way in. The list of attacks that have resulted in leaked corporate data grew longer this year: security firm RSA, marketing firm Epsilon, entertainment giant Sony, and others acknowledged breaches in 2011. Little wonder, then, that while defense-in-depth has long been a mantra of the security industry, vendors and consultants are now more strident about recommending that companies look to shore up their abilities to detect attacks that have succeeded.

(U) "When all else fails and there is some chance of the attacker getting in, the question becomes, how are we going to detect them?" says the chief technology officer for RSA and an EMC fellow. Unlike more general cybercrime, targeted and persistent attackers tend to focus on quiet reconnaissance and infiltration of their victims, making detecting the threats that much more difficult. "These things are not exploding into your network, gone are the days of your Nimdas and your Slammers," says the manager of the McAfee's Threat Intelligence Service (MTIS).

(U) To be ready for the attackers already inside the company network, security managers need to take a few steps, say experts.

(U) 1. Know The Network

(U) The most important tool in the detection drawer is a solid baseline understanding of the network. Knowing how systems are configured, how they connect, and what ports and services are available on each is a necessary step to detecting when something changes maliciously, says McAfee's MTIS manager. "If you don't know exactly how many machines are on your network, where they are, what they are doing, and how they are connected, you are absolutely exposed," he says.

(U) Companies should continually revisit their understanding of the network and the interconnected systems to incorporate changes. Checking the integrity of files is a key tool, but ensuring that configurations are hardened and follow company policy is also important, says the chief technology officer of security firm Tripwire. "Once they get in, they are in, but knowing how things looked before they got in gives you the upper hand in being able to figure out what happened and how to stop them," he says.

(U) 2. Cordon Off The Data

(U) In addition to having a comprehensive picture of the network, companies should also put their critical data in well-monitored digital "vaults." By restricting access to important data, any malicious attempts to copy or steal the data become more obvious, says the director of malware research at Dell SecureWorks. "You have to plan ahead of time," he says. "And having your sensitive data in a separate enclave where you have stricter policy enforcement is a good idea." In addition, companies can borrow a technique from insider defenses, creating honeypot or decoy files that look interesting, but result in an alarm when copied or accessed. "It is really equivalent to detecting an insider attack because the attacker is already operating from the inside," RSA's CTO says.

(U) 3. Monitor Hosts, Logs, And Network Traffic

(U) Once defenders have a baseline understanding of their networks, threats can be detected by finding anomalous behavior in log files, host behavior, and network traffic. **Companies that do not regularly examine their log files are more likely to get breached. In the latest edition of its Data Breach Investigations Report, for example, Verizon found that 69 percent of the breaches it investigated in a year could have been detected by analyzing log data.** Instead, almost seven out of every eight breaches were discovered, not by the victim, but by a third-party firm, a trend that is far less likely to happen in the case of stolen intellectual property.

(U) **Monitoring network traffic can also lead to the discovery of an attack. Moreover, systems that record network data for later analysis can help a company's analysis of a potential threat, the RSA CTO says.** "You might, in a log file, see that file XYZ has been exfiltrated," he says. "But a good attacker will delete the file, so you won't know what they took. With the packets, you can discover what was

stolen." Finally, host-based intrusion detection systems that go beyond antivirus and reactive signature detection are also key to figuring out what may be causing the anomalies -- whether a malicious attacker or a malfunctioning program. "Logs are great, network traffic is great, but those two don't give you a view of what the programs are doing," he says.

(U) Five Big Database Breaches Of 2011's Second Half; Healthcare Breaches Dominate Since the Summer, with Plenty of Lessons Learned (*Dark Reading, 14 DEC 2011*)

(U) Though the second half of the year has been comparably calmer than the first half's excitement over database breaches at RSA, Sony, and Epsilon, the breach numbers continued to roll in -- especially at healthcare organizations, which made up a disproportionate number of exposed records. Here are some of the biggest breaches that went down in the second half of the year, along with a few database security lessons learned.

(U) 1. The Breach Victim: Nemours

(U) Assets Stolen/Affected: Names, addresses, dates of birth, Social Security numbers, insurance data, medical treatment data, and bank account information for 1.6 million patients, vendors, and employees. Three unencrypted tapes containing a mother lode of personal information on patients, vendors, and employees were lost amid the dust of a facility remodel project when a cabinet that held them since 2004 went missing.

(U) Lessons Learned: Database backups are often the Achilles' heel in enterprise database security. Because of their portability and longevity, database backup tapes are frequently lost in transit or in these types of relocation scenarios. Encryption of data is key to ensuring security even when tapes can't be physically secured.

(U) 2. The Breach Victim: Tricare/SAIC

(U) Assets Stolen/Affected: Protected health information from 5.1 million patients of US military hospitals and clinics. Another day, another backup tape gone missing. In September, Tricare announced that an employee for one of its contractors, Science Applications International Corp. (SAIC), was driving around with a backup tape containing patient data from 1992 all the way through 2011 for San Antonio-area military treatment facilities. The tapes were stolen from the car, exposing Social Security numbers, addresses, phone numbers, clinical notes, lab test results, prescriptions, and other medical information.

(U) Lessons Learned: In addition to the lessons about backup tape protection, this case shows how important third-party contractor security procedures are to an organization. Enterprises and government agencies alike must be aware of how contractors are touching database information and whether they're employing best practices with regard to how that data is handled.

(U) 3. The Breach Victim: Sutter Physicians Services and Sutter Medical Foundation

(U) Assets Stolen/Affected: Personally identifiable information of 3.3 million patients supported by Sutter Physicians Services and medical information of another 934,000 Sutter Medical Foundation patients. The data in question was stolen from Sutter Medical Foundation offices when a thief made away with an unencrypted desktop computer over one weekend in October. Sutter Health is currently being sued not only for negligence in safeguarding computers and data, but also for failing to notify patients according to California state mandates.

(U) Lessons Learned: Physical security is obviously paramount in ensuring that desktops aren't made away with by cat burglars. But there are other lessons here, namely in the fact that the data was not encrypted and that such a sizable chunk was sitting on a desktop in the first place. Many enterprises today get into trouble when huge repositories of data are taken out of the database and transferred to unsecured endpoints.

(U) 4. The Breach Victim: SK Communications

(U) Assets Stolen/Affected: Thirty-five million names, email addresses, phone numbers, and resident registration numbers of social media users at South Korean sites Cyworld and Nate. In mid-July, hackers working from IP addresses originated in China infected 60 of SK Communications' computers and used that foothold to hack the company's database stores. The infections allowed them to gather enough access credentials to hack and exfiltrate data from the databases. The loot they made off with was personal information of about 90 percent of South Korean Internet users.

(U) Lessons Learned: This case shows how critical layered security, effective network segmentation, and database monitoring are to both preventing and detecting large-scale database leaks. Hackers often use malicious infections on other network devices to begin the multistep process of cracking even the most strongly fortified database infrastructure.

(U) 5. The Breach Victim: Valve, Inc.

(U) Assets Stolen/Affected: Personally identifiable information for 35 million users of Valve's online gaming site. Steam, the back-end database that runs the online video distribution site run by Valve, was compromised in November, coughing up encrypted credit card numbers and other personally identifiable information for its 35 million users.

(U) Lessons Learned: Public details of how exactly the hackers busted into Steam's database are limited, but what is interesting in this case is the bit of silver lining it offers compared to other similar breaches during the past 18 months. Though hackers did have their way with Steam's databases, risks were hugely mitigated because credit card numbers were encrypted and user passwords were salted and hashed, minimizing the impact hackers could make with the information available through their theft.
\

(U) The Most Notorious Cybercrooks Of 2011 -- And How They Got Caught; A Torrent of Attacks from Groups like Anonymous, LulzSec, Goatse Security, and Antisec has Made it a Busy Year for Cybercrime Investigators (*Dark Reading, 07 DEC 2011*)

(U) While there are plenty of elusive hackers that will forever manage to outrun the law, the good guys scored some impressive arrests, indictments, and convictions in 2011. Here are some of the highest profile cases to hit the headlines this year.

(U) 1. Anonymous and LulzSec Hacker: Ryan Cleary

(U) Police raided the home of 19-year-old Brit Ryan Cleary and arrested him this summer for allegedly using distributed denial-of-service (DDoS) attacks to take down the British Serious Organized Crime Agency (SOCA) website this year, plus websites for the International Federation of the Phonographic Industry the British Phonographic Industry last year. His arrest was heralded by authorities as part of a crackdown against LulzSec, but the loosely organized group associated with Anonymous disavowed him as its leader. Cleary for sure had some affiliation with Anonymous, though. Acrimony between him and other Anonymous members for hacking into the group's AnonOps website and exposing its members IP

addresses led to Anonymous exposing Cleary's full name, address, phone number, and IP on its site. These details were used by authorities to eventually find, arrest, and indict him.

(U) 2. Ivy League Academic Content Turbo Downloader: Aaron Swartz

(U) A programmer and fellow at Harvard University's Safra Center for Ethics, 24-year-old Aaron Swartz faced indictment this year after he downloaded more than 4 million academic articles from the Massachusetts Institute of Technology (MIT) network connection to Jstor, an online academic repository. Swartz used anonymous log-ins on the network in September 2010 and actively worked to mask his log-ins when MIT and Jstor tried to stop the massive drain of copyrighted material. After Jstor shut down access to its database from the entire MIT network, Swartz visited the campus and directly plugged in a laptop the infrastructure at an MIT networking room and left it hidden there as it downloaded more content. It was this visit in the flesh that got him nabbed; authorities had been tipped off by an IT admin about the laptop and after searching the laptop left it there along with a hidden webcam to catch Swartz when he came back for his computer. But not everyone thought his actions were criminal.

(U) 3. DNSchanger Creators: Vladimir Tsastsin, Timur Gerassimenko, Dmitri Jegorov, Valeri Aleksejev, Konstantin Poltev and Anton Ivanvov

(U) In a cybercrime bust that some security pros called one of the biggest ever, the six masterminds behind the DNSchanger malware were arrested in November for operating one of the longest running and most costly botnets to afflict the Internet. Lead by Tsastsin, this gang of thieves is accused of developing the DNSchanger malware to help perpetrate a profitable clickjacking scheme that netted it $14 million in stolen advertising views. The malware pioneered the method of using social engineering techniques to deliver unobtrusive payloads used to hijack victims' DNS settings in order to set up revenue streams based on their manipulated browsing. Law enforcement closed in on the takedown after a multiyear, public-private investigation it dubbed "Operation Ghost Click," which was initiated nearly five years ago after researchers with Trend Micro brought the gang's botnet to the attention of the Feds.

(U) 4. Sony Hacker: Cody Kretsinger

(U) This September, authorities detained and indicted Cody Kretsinger (a.k.a. "recursion") for allegedly carrying out the summer attack against Sony Pictures on behalf of LulzSec. Authorities apparently hunted down Kretsinger through the U.K.-based HideMyAss proxy server service provider he used to help him "anonymously" carry out his SQL injection attack against Sony. The provider coughed up the logs to the authorities that allowed them to match time-stamps with IP addresses to pinpoint Kretsinger as the suspect in question.

(U) 5. Anonymous' Inside Man at AT&T: Lance Moore

(U) Former AT&T Mobility contractor Lance Moore allegedly handed over to Anonymous tens of thousands of phone numbers, confidential server names with IP addresses, usernames, and passwords to log into them, plus corporate emails, presentation documents, and intellectual property that was used by the LulzSec/Antisec movement in a public data dump this summer. According to his indictment soon thereafter, his misdeeds were discovered through the robust network auditing and log management run by his employer. AT&T was able to use its various logging and intelligence capabilities to connect the dots between an AT&T VPN connection used to upload documents to FileApe.com at the same time that unauthorized access was made to sensitive information. The IP address used was assigned to a group of less than 20 contractors and further investigation by security staff showed that Moore's account was the only one used to access both FileApe and the servers with the stolen digital goods. What's more, Web

monitoring software showed that he used his account to search on Google for information on uploading files and file hosting.

(U) 6. Apple iPad Snoop: Andrew Auernheimer

(U) Authorities indicted Andrew Auernheimer (a.k.a. "weev"), a vocal member of Goatse Security, for his involvement in exposing a flaw in AT&T's Web security that the group used to acquire 114,000 email addresses belonging to iPad users, including notable celebrities, politicians, and businesspeople. The attack was carried out when Auernheimer and Goatse hackers realized they could trick the site into offering up the email address of iPad users if they sent an HTTP request that included the SIM card serial number for the corresponding device. Simply guessing serial numbers -- a task made easy by the fact that they were generated sequentially during manufacturing -- generated tons of sensitive addresses. **Auernheimer and Goatse released details about the attacks to Gawker Media, and shortly thereafter the FBI arrested Auernheimer in connection with the breach.**

(U) 7. Celebrity Hackerazzi: Christopher Chaney

(U) Celebrity-obsessed hacker Christopher Chaney took cyberstalking to a new level when he used publicly available information from celebrity blog sites to help him guess passwords to hack Google and Yahoo emails owned by 50 different stars, including Scarlett Johansson, Mila Kunis, and Christina Aguilera. Using his access he set up email-forwarding to send himself of all email received by each celebrity. Chaney was responsible for the release of nude Scarlett Johansson photos that circulated the Internet. Though FBI investigators did not release the details of exactly how they managed to track Chaney down, they did report that they were piecing the details together during an 11-month investigation they dubbed "Operation Hackerazzi."

(U) 8. Gucci Hacker: Sam Chihlung Yin

(U) Fired after being accused of selling stolen Gucci shoes and bags on the Asian gray market, the former Gucci IT employee allegedly managed to set up a VPN token using a bogus employee name on his way out the door. A forensics investigation found that after he left the job, he called the company's IT department posing as the fake employee to get his former co-workers to activate the fob, and from there he used that access to perpetrate digital mayhem, deleting servers, destroying storage set-ups ,and wiping employee mailboxes -- essentially cutting off employee access to files and email across the United States for nearly an entire business day.

(U) Workers, Technology Need To Team To Fight Insiders; Bringing Together Groups of Employees with Internal Intelligence Can Help Detect Rogue Insiders (*Dark Reading, 13 DEC 2011*)

(U) In September, US prosecutors indicted 48-year-old Chunlai Yang, a naturalized Chinese-American citizen, on charges of stealing software code and other trade secrets from his employer, trading-software firm CME Group. US authorities arrested Yang a few days before he allegedly planned to leave the United States and form a company based on the stolen technology. The incident demonstrates many of the attributes of an insider attack. Almost two-thirds of employees that commit insider theft have already accepted a position at another company or are planning to start their own firm, according to a survey of recent insider cases released last week by security firm Symantec. In addition, insiders tend to steal data that they work with every day and to which they have some feeling of entitlement, with three-quarters of incidents involving data to which the insider had access.

(U) "The entitled disgruntled thief has a belief that they own the data, even though the company is paying them," says a forensic psychologist and a co-author of the report. "They have a perception of injustice that the company has not been treating them well." In 2010, the leak of a large cache of diplomatic memos from the US Department of State through Wikileaks captured the attention of governments and companies, and shined a light on the problems of insider attacks. Now, studies of the issue might suggest better ways of tackling the prevention of insider theft and attacks.

(U) In reviewing the cases, the Symantec study found that a profile emerged of the typical intellectual-property thief. They are male with an average age of 37 years and occupy a technical position, such as scientist, engineer, programmer or sales, the study found. Trade secrets are the most common type of intellectual property stolen, accounting for about 52 percent of cases, while administrative data was taken in 30 percent of the cases and source code in 20 percent of the thefts.

(U) Defending against insider attacks is not straightforward. In the vast majority of cases, the insider steal information that they were authorized to access, making purely technical solutions ineffective. The two authors of the Symantec study believe that companies should educate their workers around the corporate intellectual-property policies and recommend that companies create a team of cross-disciplinary workers similar to the teams formed to detect signs of and prevent workplace violence. "We are advocating that these teams also start dealing with the insider threat," one of the authors says. "They are advanced in understanding worker behavior, acting as a team and rapidly coming to an analysis, if there is a problem."

(U) A second study released this week confirms many of the facets of the insider problem, but focuses on a different solution for detecting and mitigating attacks by a company's own workers. The study, conducted by the Ponemon Institute on behalf of Hewlett-Packard, found that technical and privileged users regularly access information beyond their responsibilities with little technical oversight. More than 60 percent of privileged users, typically system and database administrators, had accessed sensitive or confidential data to satisfy their curiosity. More than 40 percent of privileged users can bypass IT security, if the restriction prevent them from delivering services. "In general, a lot of the respondents admitted that they were not using a technology-based solution for govern access," says the founder and chairman of the Ponemon Institute. That's a problem, he says, because "the combination of more data, more application, and more people has made the issue of user access a mushrooming problem."

(U) A good understanding of who is accessing what is lacking in most companies, Ponemon says. More than 40 percent of companies do not have a unified view of how privileged users access data and systems across the business, according to the Ponemon study. It's a key weakness in dealing with insider attacks. Companies are setting controls and then not monitoring the security of the overall systems, says the vice president and general manager for HP's enterprise security group. "Our approach is a security intelligence platform, which focuses on how controls are working, who is actually using the access rights," he says. "You pay particular attention to sensitive data and sensitive systems."

(U) The researchers behind the Symantec study agree that companies need better intelligence to detect the potentially subtle changes in behavior that could presage an insider going rogue. "One of the things that we try to make a point of is that companies should analyze monitoring data for changes in behavior," one Stock. "Yet most companies do not have the tools to detect such changes."

(U) CYBER THREAT ITEMS FROM THE PRESS:

(U) Hackers Post Cops' Personal Data to Avenge Occupy Movement (*The Washington Times, 20 DEC 2011*)

(U) Computer hackers avenged the Occupy movement by exposing the personal information of police officers who evicted protesters and threatening family-values advocates who led a boycott of an American Muslim television show. In three December Internet postings, hackers from the loose online coalition called Anonymous published the email and physical addresses, phone numbers and, in some cases, salary details of thousands of law enforcement officers all over the country. The hackers said they were retaliating for police violence during evictions of Occupy protest camps in cities around the country, but law enforcement advocates slammed the disclosures as dangerous. "I hope the individuals behind these cyberattacks understand the consequences of what they are doing," said the president of the Federal Law Enforcement Officers Association. "There are very dangerous criminals out there who might seek retribution" against any of these police officers.

(U) Another hacker calling himself ihazcAnNONz struck the website of the Florida Family Association. The group opposes gay marriage and has promoted a successful but highly controversial boycott of advertisers on the reality TV show "All-American Muslim." The group says the show is "propaganda clearly designed to counter legitimate and present-day concerns about many Muslims who are advancing Islamic fundamentalism and Shariah law." Supporters of the show say it depicts ordinary Muslim-American families living their normal lives, and they accuse its critics bigotry. The hacker, ihazcAnNONz, warned the Florida family group, "Your hatred, bigotry and fear mongering towards Gays, Lesbians and most recently Muslim Americans has not gone unnoticed!"

(U) In an Internet posting, he told the family association he was reading its email, and he provided email addresses and partial credit-card information of two dozen or so of the group's supporters. He referred to the Occupy Wall Street movement's slogan about the "1 percent" and the "99 percent." "I am going to assume most of the people who receive your newsletter, email you and make donations are potentially part of the 99 percent ... who have been mislead by all of your [expletive] and god talk," he wrote, adding that he therefore would not post confidential information on them. The family association did not respond to an emailed request for comment.

(U) Also in December, a hacker calling himself Exphin1ty posted the email and physical addresses, phone numbers and encrypted passwords of more than 2,400 police officers and corporate security executives. "We have seen our fellow brothers and sisters being teargassed for exercising their fundamental liberal rights," he wrote. He urged fellow hackers with access to greater computing power to crack the encryption on passwords and see if the victims had used the same password for any other accounts.

(U) Websites that require users to register typically store data such as names, email addresses and passwords on their servers. Many websites encrypt passwords and credit-card details, but passwords can be decrypted with sufficient computer-processing power if users have employed a word that can be found in a dictionary. People often use the same password for multiple accounts, a practice security experts decry. "We encourage all of our [...] friends to deface and leak [the officers'] twitters, facebooks and private email accounts," Exphin1ty said.

(U) The targeted police officers and security personnel were members of the Coalition of Law Enforcement and Retail (CLEAR), a nonprofit group that promotes cooperation between local police forces and retail corporations throughout the United States. The group did not respond to an email requesting comment. A hacker called Abhaxas also posted 18,000 emails, names and passwords of customers from Specialforces.com, a website that sells military-styled clothing and weapon accessories.

A brief review suggested that many of them might be police officers or military personnel and identifiable as such by their emails. A spokesman said Specialforces.com had secured the site and alerted all its customers to the breach.

(U) Hackers under the banner "Operation Pig Roast" posted the names, phone numbers, home addresses and salaries of nearly 70 senior members of the Houston Police Department after an eviction there. However, they insisted that they did not "condone nor do we wish violent behavior against families of these officers." They claimed they got the information legally and not by hacking into websites. One computer expert said they probably broke no law. "Publishing personal details about people, if it doesn't involve hacking, is, on its face, legal," said a representative of Identity Finder, a firm that sells software to help companies secure or destroy personal data. "It's not illegal to compile and publish information that's available in public records."

(U) The senior managing director for Kroll Inc.'s cybersecurity practice, said he is seeing an increasing number of attacks aimed at illegally getting personal data from websites. He said many small- and medium-sized businesses assumed they would not be targets or wrongly thought they lacked the resources to address security questions. With "'hacktivism' growing on a global scale, it is the height of folly to presume you won't be a target," he said, referring to a term for hacker-activists. He noted that the tools for hacking website databases and for automated scanning of thousands of sites, searching for vulnerabilities, are available commercially, meaning almost anyone could accomplish this kind of computer attack. The security experts agreed that database hacking for financial rewards or just vandalism is growing even faster than politically motivated hacking, making it impossible to predict who might become a target. "People say, 'Why would they attack us?' The answer is, 'Because you've got a website,'" an expert said.

(U) Cybercrime Hits Local Government; As More Public Employees use Social Media, Mobile Devices and Cloud Computing, Cyberattacks are Becoming a Bigger Concern … Is Small-Town America Prepared? (*Governing Magazine, DEC 2011*)

(U) In August, the online group known as Anonymous hacked its way into 70 law enforcement computer systems, defacing websites and exposing sensitive information, such as email, tips on suspected crimes and profiles of gang members, according to the Associated Press. It was another example of a growing trend labeled “hacktivism,” involving activists who launch cyberprotests by targeting the computers of public- and private-sector organizations. The attack was aimed at law enforcement agencies that had been pursuing and arresting members of Anonymous.

(U) But this time the attacks didn’t occur at large federal, state or local law enforcement departments. Instead the hacktivists went after small, mostly rural police and sheriff offices. The ease with which they broke into the websites and exposed information was a strong reminder that cyberattacks can happen in any state or locality. That’s bad news for small municipalities and counties that can’t afford a chief information officer, let alone an information security chief to oversee data protection on a round-the-clock basis. Nonetheless, those same small-town agencies are increasingly running critical services on computers that can be easily shut down by hackers, cybercriminals or just a disgruntled employee.

(U) Compounding the problem is a certain lack of urgency among senior-level public officials in many local governments, large and small. While data isn’t available on how much towns, cities and counties are spending to protect information systems and prevent data breaches, a recent report by the National Association of State Chief Information Officers (NASCIO) found that 50 percent of states reported spending less than 3 percent of their IT budget on security. The private sector spends 5 percent or more. And state spending on cybersecurity is actually trending downward, according to NASCIO. Local governments are likely to show similar spending trends.

(U) Smaller local governments are also less likely to appreciate the magnitude of a cyber attack and its ramifications, says the CIO of the Public Technology Institute (PTI). “Personal data tends to be undervalued. Some municipalities don’t think they have anything to protect, since the information is considered public.” The result: less emphasis on prevention and protection. For very small governments with just a couple of servers, all it takes is one employee to open an email attachment with a virus, and the town’s entire system will be affected. “Local governments are doing so many transactions online these days, so the risk of a single virus that hits, spreads and shuts down the entire system is real,” says the city manager for Corning, New York, a municipality of 11,000 that has no IT staff of its own. “We’re reliant on these systems, so it’s a big impact when they go down.”

(U) Hacktivism is just one of a growing number of cyberthreats that governments and the information security industry are closely watching. In 2010, security firms discovered 20 million new strains of malware: botnets, viruses, worms, Trojan horses and other types of malicious software programs that can disrupt a computer, steal data, deny a website’s operation or shut down an entire network, according to PandaLabs Security. **The explosive growth in mobile devices such as smartphones and tablet PCs has increased the number of targets for cybercriminals. Other new targets arise as more people, and governments, use social media.** Sites such as Twitter and Facebook are considered trustworthy services, which makes them an even more attractive target for criminals and troublemakers. Cloud computing, in which data is stored and processed on third-party servers accessible over the Internet, has grown in popularity at all levels of government. But the Multi-State Information Sharing and Analysis Center (MS-ISAC), which assists state and local governments with cybersecurity needs, warns that cloud computing will attract new cybercriminals “who will identify new methods to infiltrate these environments and gain access to data.”

(U) Cyberthreats are becoming more nuanced and sophisticated. One such tactic goes by the name of “spear phishing.” Rather than a random attack, these email spoofs typically arrive from a trusted source and often go after a company’s trade secrets or government information. “Today’s hackers aren’t kids. They are experienced computer hackers in China or Russia,” says a cybersecurity expert. “They can get into your system and they stay in.”

(U) Yet another trend involves the ominous threat of cyberwar and its potential impact on the country’s energy grid and water supply, critical infrastructure systems that rely increasingly on information technology such as smart grids to manage these complex functions. Such e-terrorism was once considered a far-fetched fear. But recent events -- like last year’s Stuxnet virus, which infected Iran’s nuclear program -- have made these sci-fi problems a very real concern. For now, big cities, with their large-scale water treatment plants and close relationships with energy providers, have the most to worry about. But as a recent report by PTI points out, “as [energy and water] systems become increasingly interconnected and interdependent, however, the level of security for all communities is increasingly equalized.”

(U) The Corning City Manager doesn’t lose sleep over a possible Stuxnet virus entering his city’s computers. He knows that’s not the main threat. **Rather, the problem lies with the possibility of an employee doing a little Web browsing on the side that leads to trouble. Or a worker who’s tempted to open an email attachment for an offer that sounds too good to be true. Once it happens, the PC or server starts to slow down as fake error messages begin popping up, imploring the user to purchase anti-virus software that itself is another virus or botnet that can take further control of the computer.**

(U) For town and city managers without their own IT staff, the solution is to call in a third party, a specialist in cleaning up PCs, servers and networks. According to PTI’s CIO, that’s the typical response.

"The threat at the very local level is nominal for the most part and is dealt with in a reactive way, usually by calling in an IT auditor," he says.

(U) But there are a number of steps that any local government can take to prevent these types of mistakes from happening: It starts with training employees on such basics as not using government computers for personal use, not opening unrecognized email and not accessing government data via unsecured mobile devices. The PTI CIO mentions the "thumb drive test" to find out if employees are paying attention. Security audit firms will plant USB thumb drives in an organization and then see how many are turned in. Not surprisingly, a high number of employees will keep them or insert the drives into the computers, not realizing they could have launched a malware attack if the drive had been infected.

(U) Besides educating employees, local governments can prevent a great deal of computer harm by installing firewalls, backing up data, using a strong password policy, installing only approved software applications and controlling employee Internet access. But beyond the basics, what is a cash-strapped local government supposed to do to ensure its computers stay operational and protected? In the case of Corning, the city has partnered with surrounding Steuben County, which has a sizable IT staff, to be on hand to help. These types of government-to-government support services exist throughout the country, though the practice remains informal and tends to happen between small governments and their county counterparts.

(U) Meanwhile, with the next generation of computing becoming smaller and more mobile, local governments will need to revise their checklist of security precautions to include the ability to perform "remote wipes" of lost or stolen smartphones or purse-sized tablet computers. The good news is that cybercriminals have not turned their full attention to breaching iPhones, Androids and the growing variety of tablet PCs. But the security window for these devices may not last long. The proliferation of mobile devices is changing the "threat landscape," and not for the better, according to a MS-ISAC cybersecurity expert. "With more governments using mobile devices, it is making [the threat of data breaches] worse. You really have to know what to do to recover, because you will be hit."

(U) Power Problems

(U) In 2010, an ominous new type of cyber attack appeared, when the Stuxnet virus made its way into Iran's nuclear program and allegedly wreaked havoc on the country's uranium enrichment initiative. Suddenly the threat of cyberattacks on energy systems became very real. But it wasn't the first time a power grid breach had occurred. In 2009, US intelligence agencies found software left by cyberspies that had penetrated the US electrical grid. **More recently, a Texas power company found evidence that attempts to breach its grid had originated in China, according to a report by the Public Technology Institute (PTI).**

(U) While the United States has not yet suffered any damage or disruption of service to its electrical grid from cyberattacks, blackouts in 2005 and 2007 in Brazil were the result of successful attacks. A PTI report titled Cyber Security Concerns for Local Government Energy Assurance Planning points out that during the next decade, the nation's electrical grid will incorporate "numerous technologies using sophisticated computer systems and the Internet ... to improve the connectivity of electric transmission and distribution systems." Smart grids will bring significant benefits, such as increased energy efficiency, but come with a risk: vulnerability to cyberattacks.

(U) Local governments, once concerned with preparing for natural disasters, must now prepare for the consequences of cyberattacks on smart grids and other types of infrastructure, caution organizations like PTI, the US Department of Energy and the North American Electric Reliability Corporation. The PTI report urges local governments to work closely with energy utilities to identify cybersecurity risks and to

minimize threats, especially to the electrical grid since it is becoming increasingly interconnected. Once an attack occurs, what would once have been an isolated incident "could lead to a cascading power outage with wide-ranging impacts."

(U) 6 Degrees of Cybercrime; Public Officials Should Be on High Alert for These Six Threats to Cybersecurity (*Governing Magazine, DEC 2011*)

(U) At the beginning of 2011, the Multi-State Information Sharing and Analysis Center issued its annual report on cybersecurity emerging trends and threats facing state and local government. Based on the overall picture, public officials should remain on high alert.

(U) 1. Botnets and Malware: The number of new types of malicious software programs and websites reported in 2010 were in the tens of millions. Their automation and sophistication continues to increase, so expect their proliferation to continue.

(U) 2. Mobile Devices: The use of these -- and the number of applications that run on them -- continue to grow. Experts believe attacks by cybercriminals will increase significantly as they go after the operating systems that run the phones and tablet PCs.

(U) 3. Hacktivism: Cyberprotests launched by socially or politically motivated activists are on the rise. Groups such as Anonymous, Lulz Security and Operation Payback have launched spam campaigns and denial-of-service attacks against both public- and private-sector organizations.

(U) 4. Social Media: The volume of users of such sites as Twitter, LinkedIn and Facebook continues to grow exponentially. Because they are considered trustworthy sites, they are an attractive target for cybercriminals who run scams.

(U) 5. Application Vulnerabilities: Despite the growing awareness of cyberthreats, too many applications are deployed without adequate security controls, and criminals will continue to target these applications to gain access to data.

(U) 6. Cloud Computing: State and local government will expand its use of the cloud to save money and increase flexibility. Expect hackers and criminals to go where the data resides in growing volume. The report says hackers will identify new ways to infiltrate cloud platforms and access data illegally.

(U) Report Details Extent of Anonymous Hack on STRATFOR (*CNET, 27 DEC 2011*)

(U) Details are emerging about the extent of an Anonymous hack on security think tank Strategic Forecasting that was first reported Christmas Day and appears to have affected some 50,000 individuals. Austin, Texas-based Strategic Forecasting, or Stratfor, disclosed over the weekend that its Web site, which remains down, was hacked and information about its corporate subscribers--who include the likes of the US Army, US Air Force, and Miami Police Department--was disclosed. AntiSec, an Anonymous-affiliated hacktivist group, quickly claimed responsibility and promised "mayhem" with plans to release even more documents.

(U) Identity Finder, a New York-based data loss and identity theft prevention service, published a report stating that AntiSec has so far released personal information obtained in the hack for Stratfor subscribers with first names beginning with A through M. The rest of the alphabet, along with what AntiSec claims

are copies of 2.7 million e-mails, are expected to be released in upcoming days. Documents from the hack posted to date by both Anonymous and AntiSec, according to Identity Finder, include:

(U) • 50,277 unique credit card numbers, of which 9,651 are not expired
(U) • 86,594 e-mail addresses, of which 47,680 are unique
(U) • 27,537 phone numbers, of which 25,680 are unique
(U) • 44,188 encrypted passwords, of which roughly 50 percent could be easily cracked

(U) Some reports said Anonymous' stated goal was to steal money from individual accounts to give as Christmas donations to organizations like the American Red Cross and Save the Children. VentureBeat said that on Christmas Day, Anonymous had posted five receipts of donations it had made to charities using stolen cards.

(U) CNET was unable to track down Stratfor officials for comment, but a Facebook post by Chief Executive George Friedman confirms the breach, noting that the company will offer identity theft protection and monitoring services to affected subscribers. He adds that some of the people whose names were published by AntiSec had simply subscribed to the firm's publications and did not have a deeper relationship with the company.

(U) The Identity Finder CEO said credit card fraud related to the incident has already been "well documented." "This is the latest data leak by 'breachers' who not only hack into corporations but also breach their data privacy by posting the information online," Feinman said in a statement. "Unfortunately this problem will only get worse unless corporations minimize their data footprint and shrink their data target."

(U) Indeed, this is just the latest attack by Anonymous and its offshoots, who have gained notoriety for their denial-of-service attacks and data breaches on a host of targets. From Sony and the CIA to bankers, police officers, and Fox News, the attacks were, for months, almost a daily occurrence. And with the emergence of the Occupy Wall Street protests, Anonymous actions have become more organized and focused on a cause--political protest of financial inequality and corporate influence. Stratfor was likely targeted not only because of its client list of major companies and government entities but also to highlight its apparent security glitches.

(U) The "New" Biggest Threat To The Energy Industry (*MoneyMorning.com, 13 DEC 2011*)

(U) The energy industry has a dangerous enemy that is getting stronger and more motivated to damage companies' operations and wreak havoc on global oil prices. This new threat comes from the growing trend of cybercrime, and the criminals have become more focused on disrupting large industrial systems, like those operating in the energy industry. Indeed, oil companies are reporting more frequent, better organized attacks on their systems. With most of the world's energy production and distribution controlled by computers, this puts the industry in an incredibly vulnerable position.

(U) Executives say the repercussions of an attack that isn't stopped in time could be massively harmful. "If anybody gets into the area where you can control opening and closing of valves, or release valves, you can imagine what happens," an IT manager at Royal Dutch Shell PLC, said at the World Petroleum Congress in Doha, Qatar. "It will cost lives and it will cost production, it will cost money, cause fires and cause loss of containment, environmental damage - huge, huge damage."

(U) Crime Targets the Energy Industry

(U) **Cybercrime used to focus on hacking into systems to retrieve people's personal financial information. But now it's become more sophisticated and hackers more skilled, targeting more complex and protected systems to get highly classified information.** "The scene used to be dominated by speculative attacks - people being at the wrong place at the wrong time, but it was nothing personal," a security researcher told BBC News. "But we certainly are in a different world than where we were 18 months ago. What we're starting to see is an increase in targeted attacks. We know critical systems, like those in oil production, are vulnerable to attack."

(U) The Shell IT manager told Reuters hackers are now unleashing attacks over longer periods of time, collecting more information than before to create more complex and resilient infections. While other businesses can more easily shut down their information technology systems to update software security, the energy industry cannot simply turn off the oil and gas supply for long stretches of time. Any long disruption, from an attack or from trying to prevent one, wouldn't just affect one company, but the entire global oil market. "Oil needs to keep on flowing," the head of IT security at Abu Dhabi Co. for Onshore Oil Operations, told Reuters. "We have a very strategic position in the global oil and gas market. If they could bring down one of the big players in the oil and gas market you can imagine what this will do for the oil price - it would blow the market."

(U) The energy industry became of aware of how far cybercrime has progressed when Stuxnet, a highly sophisticated piece of malware, was detected in June 2010. Stuxnet is believed to be the first worm created to target high value infrastructure like power stations and water plants. Stuxnet differs from most viruses in that it targets systems that commonly aren't connected to the Internet for security purposes. Instead it infects through keys used to move files around. After it infects the machine and can access a company's internal network, it hunts for specific software made by Siemens AG. Stuxnet can then reprogram the software and give new instructions to the machinery it controls. The Stuxnet virus crippled Iran's computers, putting the country's plan for atomic weapons at least two years behind schedule.

(U) Stuxnet made the energy industry aware that an attack on their systems was not only possible but likely. Now it's one of their biggest concerns. "It's something that we have to stay on top of every day," the director of International Government Relations at Canada-based global energy company Nexen Inc. told Reuters. "It is a risk that is only going to grow and is probably one of the preeminent risks that we face today and will continue to face for some time." The frightening truth is that with hackers able to operate from anywhere in the world, and becoming harder to detect, the industry is getting closer to a dangerous cyberattack. In fact, security software maker Symantec Corp. in October published a report on a new virus similar to Stuxnet, named Duqu. Duqu appears to be designed to gather information that makes it easier to launch future attacks. "So far we haven't had any major incidents," said Abu Dhabi Co.'s IT security head. "But are we really in control? The answer has to be "no."'

(U) Espionage Hack Attack Preys on Chemical Firms; Spotted in the Wild: Nitro Part II
(www.theregister.co.uk, 12 DEC 2011)

(U) More than two months after the discovery of an organized malware campaign targeting dozens of companies in the defense and chemical industries, the espionage hack attack shows no signs of letting up. According to a blog post published in December, the same group that targeted at least 38 companies between July and September is continuing its assault with emails that attempt to trick recipients at sensitive companies into installing backdoor trojans on their employer-issued computers. **In the latest iteration, the emails contain a malicious attachment of the very document Symantec issued in late October warning of the so-called Nitro attacks.**

(U) “Despite the publishing of the whitepaper, this group persists in continuing their activities unchecked,” two Symantec researchers wrote. “They are using the exact same techniques – even using the same hosting provider for their command and control (C&C) servers.”

(U) The domains used in the attacks have been disabled, and Symantec officials have contacted the hosting providers used in the attacks. The company's email scanning service continues to block the malicious messages. **December's report comes two months after Symantec warned that dozens of companies in the defense and chemical industries had been hit by attacks that installed a variant of the publicly available Poison Ivy backdoor trojan on network-connected PCs**. Once installed, the program uploaded proprietary data to servers under the control of attackers. Symantec said at the time that it disrupted the campaign in the middle of September. The latest report didn't say how the attackers were able to revive the attack. The Symantec report came around the same time that an IT manager for Shell told the World Petroleum Conference that the industry is experiencing an uptick in online attacks. “We see an increasing number of attacks on our IT systems and information and there are various motivations behind it – criminal and commercial.”

(U) The most recent email (Figure 1) brazenly claims to be from Symantec and offers protection from “poison Ivy Trojan”!

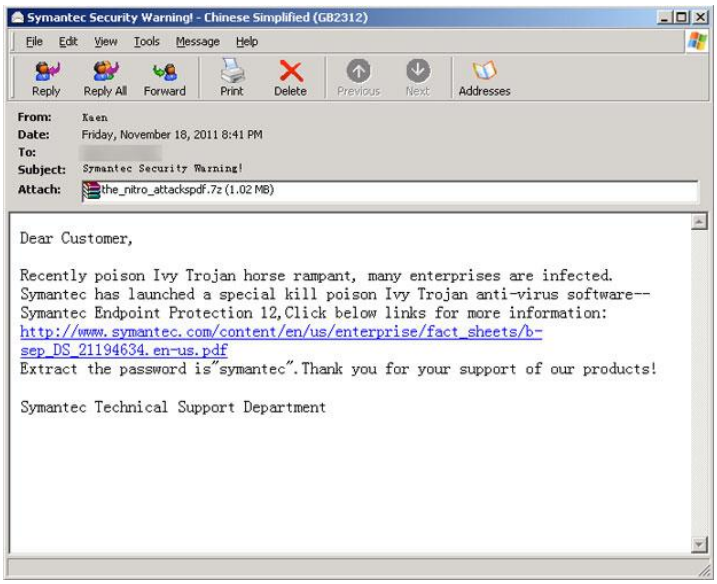


Figure 1 Fake malicious email

Furthermore, the attachment itself is called “the_nitro_attackspdf.7z”. The attachment archive contains a file called “the_nitro_attackspdf .exe”. (The large gap between the “pdf” and “.exe” is a basic attempt to fool a user into assuming that the document is a PDF, when it is really a self-extracting archive.)

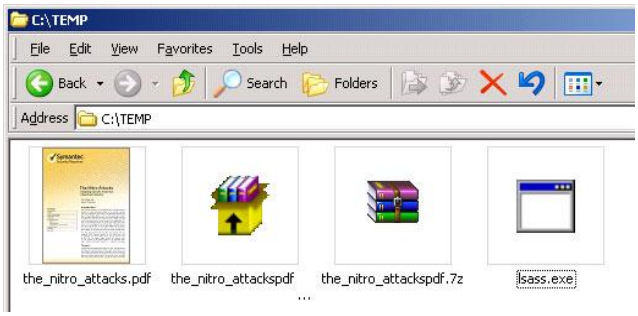


Figure 2 Contents of the attachment, including the genuine report

(U) When the self-extracting executable runs, it creates a file called lsass.exe (Poison IVY) and creates a PDF file. This PDF file is none other than our own Nitro Attacks document! The attackers, in an attempt to lend some validity to their email, are sending a document to targets that describes their very own activity.

(U) The threat, lsass.exe, copies itself to "%System%\web\service.exe" and attempts to connect to the domain "luckysun.no-ip.org". This domain resolves to an IP, which is hosted by the same hosting provider that hosted most of the previously encountered IP addresses. Figure 3 is a partial graph of the domains involved, including the most recent activity.

Figure 3 Network map

Table 1 lists the latest emails intercepted by Symantec .cloud and the MD5s of the associated threat samples.

Subject	File name	MD5	Detection
Symantec Security Warning!	The_nitro_attackspdf .exe	90e793e64e63317db15f4a64be8b56f9	Trojan.ADH

so funny	123.doc.exe	0b1b0fe45a179f75a5c4c3bad21ca185	Backdoor.Bifrose
N/A	learning materials.doc .exe	eb404fe1eec399127ac39336427503ac	Backdoor.Bifrose
adobe update	Adobe Reader Update.exe	d3ee44d903876bd942fc595c96151df8	Trojan.ADH
Adobe Reader Upgrade Rightnow!	Install_ reader10_en_air_gtbd_aih.exe	d6404d5c7a65a23d8d1687fe1549d21e	Backdoor.Odivy
Safety Tips	Q329834_WXP_SP2_ia364_ENU.exe	14c9d01d152e25e98e6ee8758ecfa9a8	Trojan.Dropper

Table 1 most recent emails and samples

Despite the publishing of the whitepaper, this group persists in continuing their activities unchecked. They are using the exact same techniques - even using the same hosting provider for their command and control (C&C) servers. The domains have been disabled and Symantec have contacted the relevant IP hosting provider and continue to block the emails through the .cloud email scanning service. Symantec.cloud customers have been and continue to be protected from attacks performed by this group.

(U) Analyst Comment: This article highlights the APT threat and the level of sophistication that state-sponsored hackers are using to craft spearphishing emails, in this case creating an email with malware that looks like it was sent from an anti-virus company to combat an APT! All companies should create and implement robust information security training programs.

(U) Homeland Security Warns SCADA Operators of Internet-Facing Systems (*www.threatpost.com*, *12 DEC 2011*)

(U) In the wake of the hack of water and sewer infrastructure operated by a Texas community, the Department of Homeland Security is again warning owners and operators of critical infrastructure to take note of SCADA and industrial control systems that may be accessible from the Internet. DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reiterated a warning from last year that such systems can be detected by a new breed of Internet scanners such as Sh0dan, citing an "uptick in related activity" by researchers, and evidence that "thousands" of ICS systems may be discoverable.

(U) ICS CERT is urging ICS asset owners and operators to audit the configuration of their systems and make sure they cannot be discovered using an Internet based scanning tool. The warning comes weeks after an unknown hacker using the handle "pr0f" claimed responsibility for the compromise of a sewage treatment system operated by the community of South Houston, Texas. In an interview with Threatpost, pr0f said that he used a custom-built scanner that searched for systems running Siemens Simatic HMI (Human Machine Interface) software and that was accessible from the public Internet. After finding such a system operated by South Houston, pr0f was able to access it by breaking a three character password used to secure an administrative account.

(U) The ICS-CERT warning lists five reports so far in 2011 of SCADA and ICS systems exposed using scanners like Sh0dan or similar tools. Though South Houston is not mentioned by name, the alert does describe a November incident in which an individual accessed an Internet facing control system using the default user name and password which is almost identical to the South Houston hack. It also calls attention to a September report by independent researcher Eireann Leverett of "several thousand" Internet devices discovered using Sh0dan. Typically, industrial control systems are given access to the Internet so that they can be remotely managed and monitored, the alert says. Unfortunately, critical infrastructure

operators frequently fail to secure such systems using a firewall or even hardened user name and password, making them easy prey for malicious hackers.

(U) In an article for Threatpost in November, 2010, the Sh0dan creator said that his tool was "just scratching the surface of unprotected or misconfigured SCADA devices." "Since it mostly looks for computers running a web server, it misses any device that relies on a custom daemon operating on a different port. That doesn't mean that such systems are undiscoverable. It just means that Shodan isn't looking for them. And, of course, the search engine merely finds systems. It doesn't expose the myriad of bad security practices that seem to be rampant amongst vendors and operators." He advised SCADA system owners and operators to take a few, simple security precautions such as deploying security around the critical systems in layers that include virtual private network (VPN) software for remote access, strong passwords, firewall, and hardening of the device itself.

(U) Power Grid Cybersecurity: Who's In Charge? (*Tech News World, 16 DEC 2011*)

(U) A country or region's power supply can be a juicy target for cyberattack, especially if it's made part of a larger assault. Is the United States' grid adequately protected? Studies on the matter have raised serious doubts. Millions of new so-called smart electric devices could introduce new options for attack that may result in a loss of control over the grid. Cybersecurity experts have been murmuring for some time that the United States' power supply is open to cyberattacks. "If someone were to think about attacking another nation, the first thing they'd do is take out the power grid, since it's the hub around which other infrastructure spokes revolve," the president and CEO of the National Electric Sector Cybersecurity Organization (NESCO), told TechNewsWorld.

(U) A recently released MIT study seems to be bringing matters to a head. Among other things, the report calls for the establishment of one organization to head cybersecurity efforts for the US power infrastructure. It states that, essentially, there are far too many organizations overseeing different aspects of power supply cybersecurity. The report followed news in early November that someone had hacked into a small water-utility serving Springfield, Ill., from Russia. The United States Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has since stated there was no evidence of a cyber intrusion into the utility's SCADA system or, essentially, that anything bad had happened.

(U) What's going on with our power supply? Too Much Information

(U) Advances in technology such as new so-called smart meters utilities have contributed to the cybersecurity mess dogging America's power supply. Millions of new communicating electronic devices, from automated meters to synchrophasors, will introduce new options for attack that could result in anything from loss of control over grid devices to loss of communications between utilities or control centers, or even blackouts, the MIT study found. Over the next 20 years, the growth of data flowing through grid communications networks will far exceed that of electricity flowing through the grid in percentage terms, the study said. In other words, if the amount of electricity grows by x percent, the amount of data would be a multiple of x.

(U) Many Hands Don't Make Light Work - Another part of the problem is that nobody's in charge.

(U) Two bills, S. 1342 and H.R. 5026, were introduced in Congress, the report states. Both propose a single agency to oversee cybersecurity for the electric power system. However, the Obama administration seems to want to put Homeland Security in charge, while Congress is opting for the Department of Energy and the Federal Energy Regulatory Commission. That split is evident lower down in the food chain. FERC has the responsibility for adopting standards under the Energy Independence and Security

Act of 2007, but the US Government Accountability Office, according to the study, has found that FERC lacks an approach to monitor industry compliance to standards it adopts.

(U) The main regulations governing grid cybersecurity are the North American Electric Reliability Corporation (NERC)'s Critical Infrastructure Protection standards. However, the National Institute of Standards and Technology (NIST) offers its own set of guidelines that are more wide-ranging and technical in nature than those from NERC. Although the two sets of standards may not overlap substantially because of their different areas of focus, their very existence might create confusion. The Federal Communications Commission has identified the potential for conflict between the CIP and other standards and said the resulting ambiguity was slowing utilities' decision making and deployment of new technologies.

(U) Responsibility Without Authority

(U) Further, standards-setting organizations such as NIST don't have the muscle to ensure adherence to their recommendations. "NIST was legislatively given responsibility for coordinating the development of standards but does not have regulatory or operational authority," a research affiliate with the MIT Energy Initiative, which conducted the study on cybersecurity in the nation's power system, told TechNewsWorld.

(U) There Can Only Be One

(U) "We believe that what is most important is that it be made clear that some agency is in charge across all aspects of the grid, including the bulk power system, currently regulated by FERC, and the investor-owned distribution system, which includes cooperative and municipal distribution systems, currently regulated by individual state public utility commissions," MIT's research affiliate said. Improving cybersecurity will "require a coordinated approach to standards and regulation across all aspects of this increasingly interconnected grid," he cautioned. The confusion may be exacerbated by internecine disputes. An audit earlier this year by the DoE inspector-general criticized FERC for approving CIP standards that didn't contain commonly used security practices and adopted a poor approach to implementation, the MIT study asserted.

(U) What About SCADA?

(U) Another important part of the power infrastructure, supervisory control and data acquisition (SCADA) control systems, is often ignored in conversations about cybersecurity. As a rule, SCADA systems tend not to be protected. "This is just an area of industry that simply had not experienced the level of scrutiny that, say, makers of desktop applications or operating systems had faced, so they had never created a process or internal dedicated teams to deal with the issue," the CEO of RedSeal Networks, told TechNewsWorld. "When it came to protecting clients in a number of instances, the advice from vendors was to unplug the SCADA solution from anything connected to the Internet or any public network," he added.

(U) Things are changing for the better, partly because of growing pressure from regulators. Still, "it's a big problem where you have old systems, sometimes unresponsive vendors, limited resources and yet [a technology that's] a tremendous source of risk to almost everyone," the CEO stated. Few in the power-generation industry really understand supervisory control and data acquisition (SCADA) control systems, a managing partner at Applied Control Solutions, who's an expert on control systems security, told TechNewsWorld. "We don't have enough people who even know what the problem is," he explained. "How the heck can we have a plan when we don't know what the problem is?"

(U) Cyber Attacks Could Wreck World Oil Supply (*Reuters, 08 DEC 2011*)

(U) Hackers are bombarding the world's computer controlled energy sector, conducting industrial espionage and threatening potential global havoc through oil supply disruption. Oil company executives warned that attacks were becoming more frequent and more carefully planned."If anybody gets into the area where you can control opening and closing of valves, or release valves, you can imagine what happens," said Ludolf Luehmann, an IT manager at Shell Europe's biggest company . "It will cost lives and it will cost production, it will cost money, cause fires and cause loss of containment, environmental damage - huge, huge damage," he told the World Petroleum Congress in Doha.

(U) Computers control nearly all the world's energy production and distribution in systems that are increasingly vulnerable to cyber attacks that could put cutting-edge fuel production technology in rival company hands. "We see an increasing number of attacks on our IT systems and information and there are various motivations behind it - criminal and commercial," said Luehmann. "We see an increasing number of attacks with clear commercial interests, focusing on research and development, to gain the competitive advantage."

(U) He said the Stuxnet computer worm discovered in 2010, the first found that was specifically designed to subvert industrial systems, changed the world of international oil companies because it was the first visible attack to have a significant impact on process control. But the determination and stamina shown by hackers when they attack industrial systems and companies has now stepped up a gear, and there has been a surge in multi-pronged attacks to break into specific operation systems within producers, he said.

"Cyber crime is a huge issue. It's not restricted to one company or another it's really broad and it is ongoing," said the director of International Government Relations at Canada's Nexen Inc. "It is a very significant risk to our business." "It's something that we have to stay on top of every day. It is a risk that is only going to grow and is probably one of the preeminent risks that we face today and will continue to face for some time." Luehmann said hackers were increasingly staging attack over long periods, silently collecting information over weeks or months before attacking specific targets within company operations with the information they have collected over a long period. "It's a new dimension of attacks that we see in Shell," he said.

(U) Not in Control

(U) In October, security software maker Symantec Corp said it had found a mysterious virus that contained code similar to Stuxnet, called Duqu, which experts say appears designed to gather data to make it easier to launch future cyber attacks. Other businesses can shut down their information technology (IT) systems to regularly install rapidly breached software security patches and update vulnerable operating systems. But energy companies cannot keep taking down plants to patch up security holes. "Oil needs to keep on flowing," said the head of IT security at Abu Dhabi Company for Onshore Oil Operations (ADCO). "We have a very strategic position in the global oil and gas market," he added. "If they could bring down one of the big players in the oil and gas market you can imagine what this will do for the oil price - it would blow the market."

(U) Hackers could finance their operations by using options markets to bet on the price movements caused by disruptions, said the ADCO IT security head. "So far we haven't had any major incidents," he said. "But are we really in control? The answer has to be 'no'." Oil prices usually rise whenever tensions escalate over Iran's disputed nuclear program - itself thought to be the principal target of the Stuxnet worm and which has already identified Duqu infections - due to concern that oil production or exports from the Middle East could be affected by any conflict.

(U) But the threat of a coordinated attack on energy installations across the world is also real, experts say, and unlike a blockade of the Gulf can be launched from anywhere, with no US military might in sight and little chance of finding the perpetrator. "We know that the Straits of Hormuz are of strategic importance to the world," said the vice president of oil and gas operations in the Middle East and North Africa for business application software developer SAP. "What about the approximately 80 million barrels that are processed through IT systems?," he said. Attacks like Stuxnet are so complex that very few organizations in the world are able to set them up, the chief security officer at Germany's SAP said, but it was still too simple to attack industries over the internet.

(U) Only a few years ago hacking was confined to skilled computer programmers, but thanks to online video tutorials, breaking into corporate operating systems is now a free for all. "Everyone can hack today," Shell's Luehmann said. "The number of potential hackers is not a few very skilled People, it's everyone."

(U) Healthcare Data In Critical Condition; New Study Shows Data Breaches Increasing and Costing Healthcare Industry Billions of Dollars a Year, with Employees, Mobile Devices the Weakest Links (*Dark Reading, 01 DEC 2011*)

(U) A new report taking the pulse of the healthcare industry finds that data breaches have jumped more than 30 percent and could be costing the industry an average of $6.5 billion annually. **The new Ponemon Institute "2011 Benchmark Study on Patient Privacy and Data Security," commissioned by IDExperts, found that employee error is one of the main reasons for data breaches in hospitals and healthcare providers.** Hospitals and healthcare providers suffered an average of four data breaches in the past year, according to the report.

(U) But the jump in breaches is, in part, due to better detection capabilities by healthcare organizations, says the chairman and founder of the Ponemon Institute. "It was not too surprising that the rate of data loss increased … [But] we think that finding may not be as negative as it appears, and could be a discovery-rate increase with more control and governance practices and use of enabling technologies." Another big factor in data loss, however, is the explosion in mobile devices in the healthcare field. Some 80 percent employ these devices for gathering, transmitting, and storing patient information, but half are not securing them. While these devices help patient care, they also pose a major risk of exposure for the patient's health and other personal information, the Ponemon chairman says.

(U) "With all of the focus around HIPAA and HITECH [Act] and security, it surprised me to see these organizations would allow the deployment of those devices [unsecured]," says the president of ID Experts. "It's like people driving the Indy 500 without seatbelts." Among the top reasons for breaches: nearly half were stolen or lost computing or data devices, and 46 percent, due to third-party provider mistakes. Another problem is knowing just where patient data resides: Sixty-one percent say they are "not confident" they know where all patient data is being stored. More than half aren't sure they can detect incidents of data exposure.

(U) More than 80 percent of hospitals have written policies for data breach reporting, but nearly 60 percent say the policies are ineffective. More than 40 percent say administrative employees are least cognizant of the need for protecting patient information. Nearly 30 percent say the breaches they suffered resulted in medical identity theft, a more than 25 percent increase over 2010.

(U) Hospital Turns Away Patients After "Virus" Disrupts Network; Another Worm Attack? (*Techworld, 12 DEC 11*)

(U) A US hospital had to turn away patients in December after being hit by a "virus" infection that downed the institution's network and sent staff back to using paper records. The unidentified malware started to cause problems for the Gwinnett Medical Center in Lawrenceville Georgia on a Wednesday and got progressively worse until the hospital was forced to divert all non-emergency admissions to other medical centers. By Friday night, the IT team had the outbreak under control and by Saturday were able to go back to using the computerized records system, local media reported.

(U) The source of the outbreak, not the first that has affected the hospital according to sources, is still not clear, nor has the malware been identified beyond it being described generically as a "virus." "We actually have some of our IT vendor partners that are on site with us that have actually been here since Wednesday. We've also got internal teams that are trying to identify the virus issues," said a Gwinnett Medical Center spokesperson. "It's not affecting patient care in any way, shape or form," she said adding that patient data had not been at risk.

(U) Given the symptoms mentioned in reports, a worm infection (for example by Conficker or one of its variants) seems the most likely cause, which could have spread rapidly across the hospital's network forcing IT to pull connectivity to avoid it spreading further with unknown consequences. The standard procedure for a fast-spreading worm is immediate isolation followed by a hunt for the point at which the malware entered the network, most likely a laptop or USB stick brought into the hospital by a member of staff.

(U) The events bear a striking resemblance to a similar problem that recently hit New Zealand's St John Ambulance Service. That attack disrupted the ambulance communications system, forcing administrators to revert to manual radio contact to direct staff to emergencies. As with any organization using Windows-based PCs, hospitals are regularly afflicted with malware but it is still unusual for institutions to find themselves disrupted seriously enough for the fact to become public.

(U) In 2008, admissions systems at three hospitals in London had to be shut down after 4,700 computers became infected with the Mytob worm first detected by security companies three years earlier. A security report on the incident later described the worm infection as "entirely avoidable," and as having been caused by a number of factors including poor management of antivirus updates on the affected machines. Mytob acquired a reputation for potency. In a separate discovery, a variant was found that spread by posing as a message from the IT administrator.

(U) Three Bulgarians Arrested in Connection With Phishing Scheme Against US Banks (*IDG News Service, 13 DEC 2011*)

(U) Bulgarian authorities have arrested three men on charges of being part of an international cybercriminal gang that targeted US bank customers. The men were detained last week in Sofia and Burgas following a joint investigation by the computer crime division of the Bulgarian Chief Directorate for Combating Organized Crime (CDCOC) and the FBI.

(U) The gang sent phishing emails that appeared to originate from major US banks and directed recipients to fake online banking websites with the purpose of stealing their user names and passwords, the Bulgarian Interior Ministry said in a statement last week. The men's names were not given and their ages were described only as "between 28 and 36." The men allegedly used the stolen information to transfer money from bank accounts belonging to victims. Investigators said that the three suspects used online

payment services such as libertyreserve.com, paypal.com, webmoney.ru, moneybookers.com and others. During raids at the three men's homes police officers seized mobile phones, computer systems containing hacking programs, laptops, storage media devices, receipts of numerous money transactions, as well as stolen online banking credentials. The suspects will be charged with financial crimes.

(U) The law enforcement operation resulting in these arrests took place on Dec. 7, one day before FBI Director Robert Muller arrived in Sofia to meet with Bulgarian Prime Minister Boyko Borisov, Interior Minister Tsvetan Tsvetanov and the directors of the country's security structures. Combating cybercrime was a major focus of the discussions Muller had with the Bulgarian officials, the country's Interior Ministry announced. Muller said that he hopes the FBI and the CDCOC will collaborate more.

(U) As Few as 12 Hacker Teams Responsible for Bulk of China-Based Data Theft (*Associated Press, 12 DEC 2011*)

(U) As few as 12 different Chinese groups, largely backed or directed by the government there, commit the bulk of the China-based cyberattacks stealing critical data from US companies and government agencies, according to US cybersecurity analysts and experts. The aggressive but stealthy attacks, which have stolen billions of dollars in intellectual property and data, often carry distinct signatures allowing US officials to link them to certain hacker teams. Analysts say the United States often gives the attackers unique names or numbers, and at times can tell where the hackers are and even who they may be.

(U) Sketched out by analysts who have worked with US companies and the government on computer intrusions, the details illuminate recent claims by American intelligence officials about the escalating cyber threat emanating from China. And the widening expanse of targets, coupled with the expensive and sensitive technologies they are losing, is putting increased pressure on the United States to take a much harder stand against the communist giant. It is largely impossible for the United States to prosecute hackers in China, since it requires reciprocal agreements between the two countries, and it is always difficult to provide ironclad proof that the hacking came from specific people.

(U) Several analysts described the Chinese attacks, speaking on condition of anonymity because of the sensitivity of the investigations and to protect the privacy of clients. China has routinely rejected allegations of cyberspying and says it also is a target. “Industry is already feeling that they are at war,” said James Cartwright, a retired Marine general and former vice chairman of the Joint Chiefs of Staff. A recognized expert on cyber issues, Cartwright has come out strongly in favor of increased US efforts to hold China and other countries accountable for the cyberattacks that come from within their borders. “Right now we have the worst of worlds,” said Cartwright. “If you want to attack me you can do it all you want, because I can’t do anything about it. It’s risk-free, and you’re willing to take almost any risk to come after me.” The United States, he said, “needs to say, if you come after me, I’m going to find you, I’m going to do something about it. It will be proportional, but I’m going to do something ... and if you’re hiding in a third country, I’m going to tell that country you’re there. If they don’t stop you from doing it, I’m going to come and get you.”

(U) Cyber experts say companies are frustrated that the government isn’t doing enough to pressure China to stop the attacks or go after hackers in that country. Much like during the Cold War with Russia, officials say the United States needs to make it clear that there will be repercussions for cyberattacks. The government “needs to do more to increase the risk,” said the head of the counter threat unit at the Atlanta-based Dell SecureWorks, a computer security consulting company. “In the private sector we’re always on defense. We can’t do something about it, but someone has to. There is no deterrent not to attack the United States.”

(U) Cyberattacks originating in China have been a problem for years, but until a decade or so ago analysts said the probes focused mainly on the US government — a generally acknowledged intelligence gathering activity similar to Americans and Russians spying on each other during the Cold War. But in the last 10 to 15 years, the attacks have gradually broadened to target defense companies, then other critical industries, including energy and finance. According to Dell SecureWorks head and other cyber analysts, hackers in China have different digital fingerprints, often visible through the computer code they use, or the command and control computers that they use to move their malicious software. US government officials have been reluctant to tie the attacks directly back to the Chinese government, but analysts and officials quietly say they have tracked enough intrusions to specific locations to be confident they are linked to Beijing — either the government or the military. They add that they can sometimes glean who benefited from a particular stolen technology.

(U) **One of the analysts said investigations show that the dozen or so Chinese teams appear to get "taskings," or orders, to go after specific technologies or companies within a particular industry. At times, two or more of the teams appear to get the same shopping list and compete to be the first to get them or to pull off the greatest haul. Analysts and US officials agree that a majority of the cyberattacks seeking intellectual property or other sensitive or classified data are done by China-based hackers. Many of the cyberattacks stealing credit card or financial information come from Eastern Europe or Russia.**

(U) According to experts, the malicious software or high-tech tools used by the Chinese haven't gotten much more sophisticated in recent years. But the threat is persistent, often burying malware deep in computer networks so it can be used again and again over the course of several months or even years. The tools include malware that can record keystrokes, steal and decrypt passwords, and copy and compress data so it can be transferred back to the attacker's computer. The malware can then delete itself or disappear until needed again.

(U) Several specific attacks linked to China include:

(U) — Two sophisticated attacks against Google's systems stole some of the Internet giant's intellectual property and broke into the Gmail accounts of several hundred people, including senior US government officials, military personnel and political activists.

(U) — Last year, computer security firm Mandiant reported that data was stolen from a Fortune 500 manufacturing company during business negotiations when the company was trying to buy a Chinese company.

(U) — Earlier this year, McAfee traced an intrusion to an Internet protocol address in China and said intruders took data from global oil, energy and petrochemical companies.

(U) A Chinese Foreign Ministry spokesman, Liu Weimin, did not respond Monday to the specific allegations about government-supported cyber-attacks but said Internet security is an issue the world needs to address collectively. The international community should "prevent the Internet from becoming a new battlefield," Liu said at a daily media briefing in Beijing.

(U) **For the first time, US intelligence officials called out China and Russia last month, saying they are systematically stealing American high-tech data for their own economic gain. The unusually forceful public report seemed to signal a new, more vocal US government campaign against the cyberattacks.** The next step, said Cartwright, must be a full-throated US policy that makes it clear how the United States will deal with cyberattacks, including the attackers as well as the nations the attacks are routed through. Once an attack is detected, he said, the United States should first go through the State

Department to ask the country to stop the attack. If the country refuses, he said, the United States will have the right to stop the computer server from sending the attack by whatever means possible while still avoiding any collateral damage.

(U) Adobe Zero-Day Exploit Targeted Defense Contractors; Adobe Credits Lockheed Martin, Victim of Earlier Attack, and Defense Industry Cyber-Threat Group with Reporting Unpatched Bug (*Eweek, 07 DEC 2011; Computerworld, 06 DEC 2011*)

(U) Researchers found samples of malicious PDF files exploiting the recently disclosed Adobe zero-day vulnerability that were sent to defense contractors and other organizations. Attacks exploiting an Adobe Reader zero-day vulnerability appear to have targeted defense contractors and other organizations, according to security researchers. Adobe issued a security advisory on Dec. 6 warning Adobe Reader and Acrobat users of a critical vulnerability in how the programs accessed PDF files. The flaw was also being exploited in the wild against Adobe Reader 9.x users on Windows, Adobe said.

(U) Symantec researchers found that attack emails with malicious PDF files that exploited the flaw were sent to telecommunications and chemical companies as well as defense contractors, a security intelligence manager of Symantec Security Response, told eWEEK. The emails had been spoofed to look like they were sent from agencies and organizations that were familiar to the recipients, he said. Symantec security researchers found attack emails from Nov. 1 and Nov. 5 that exploited the vulnerability, a security response engineer at Symantec, wrote on the Symantec Security Response blog Dec. 7. Attackers used "social engineering to trick users into opening the file," he said.

(U) **Lockheed Martin and the Defense Security Information Exchange were credited for bringing the vulnerability to Adobe's attention, according to the security advisory. The DSIE is a group of major defense contractors that are part of the Defense Industrial Base and share information about computer attacks with each other.** DIB members include Boeing, General Dynamics, Lockheed Martin, Northrop Grumman, Pratt & Whitney and Raytheon. The attackers were sophisticated, customizing the attack for each victim, as they crafted different PDF files and attack emails to specifically target each organization, the Symantec intelligence manager said. "Someone in the communications industry is likely to receive a different email and PDF file than someone in a manufacturing company would," he said.

(U) Adobe issued a security advisory with what information it was willing to share. Adobe acknowledged that the vulnerability is being exploited in what it called "limited, targeted attacks" against Reader 9.x on Windows, but did not provide any additional information about where and when the attacks were occurring, or who had been targeted. Adobe identified the bug as a "U3D memory corruption vulnerability," U3D, which stands for "universal 3D," is a compressed file format standard for 3-D graphics data promoted by a group of companies, including Adobe, Intel, and Hewlett-Packard.

(U) While a patch for Reader and Acrobat 9 will reach users in December, Adobe said it will not deliver fixes for Reader and Acrobat 10 for Windows, as well as all versions for Mac OS X and Unix, until Jan. 10, 2012. Adobe justified those delays on the grounds that Reader 10, also called Reader X, includes anti-exploit "sandbox" technology that isolates the application from the rest of the computer, and thus blocks the exploit now in circulation. The company said that the risk to Macintosh and Unix users was "significantly lower" because attacks have been spotted targeting only Windows PCs.

(U) Lockheed Martin is one of the United States' largest aerospace and defense contractors, and manufactures the F-22 Raptor fighter jet and won the contract to build the F-35 Lightning II, the planned successor to the F-16 Falcon aircraft. MITRE manages several research centers funded by US government agencies, including the National Security Engineering Center for the Department of Defense,

and the Center for Advanced Aviation System Development for the Federal Aviation Administration (FAA).

(U) Analyst Comment: This article highlight the value in private companies sharing information with other companies and with the FBI.

(U) Advanced Persistent Threats (APTs) Expected to Grow in Volume and Sophistication, Warns Fidelis Chief (*19 DEC 2011, infosecurity.com*)

(U) Nation-state-sponsored advanced persistent threats (APTs) are only going to increase in volume and sophistication over the next few years, and the US needs to take the offense in countering these threats, argues the president and chief executive officer of network security firm Fidelis. Because nation-states are well funded and organized, they are able to carry out very sophisticated, content-based attacks that are hard to detect and to stop, he told Infosecurity.

(U) The Fidelis chief noted that APTs are often embedded deep inside content. So tools to discover and stop these threats need to provide content-level visibility. He estimated that 90 percent of the companies being attacked by APTs do not have this content-level visibility. "Nation-states are burying malware deep inside the content, and the companies can't see that….We see the threat vector continuing and the amount of content-based malware going up dramatically over the next couple of years", he predicted.

(U) Fidelis works closely with federal government customers, the CEO noted. "We are seeing an increasing desire from the national security leadership to be more overt about delivering the news to the world that we have technology and capabilities to not only be world-class in defense, but more important to be world-class in offense", he said. China "needs to know that we are going to be very aggressive on the offensive side to deal with their offensive attacks on our national security. It is not acceptable to steal classified information. It is not acceptable to attack our intellectual property and use that for profit", he said.

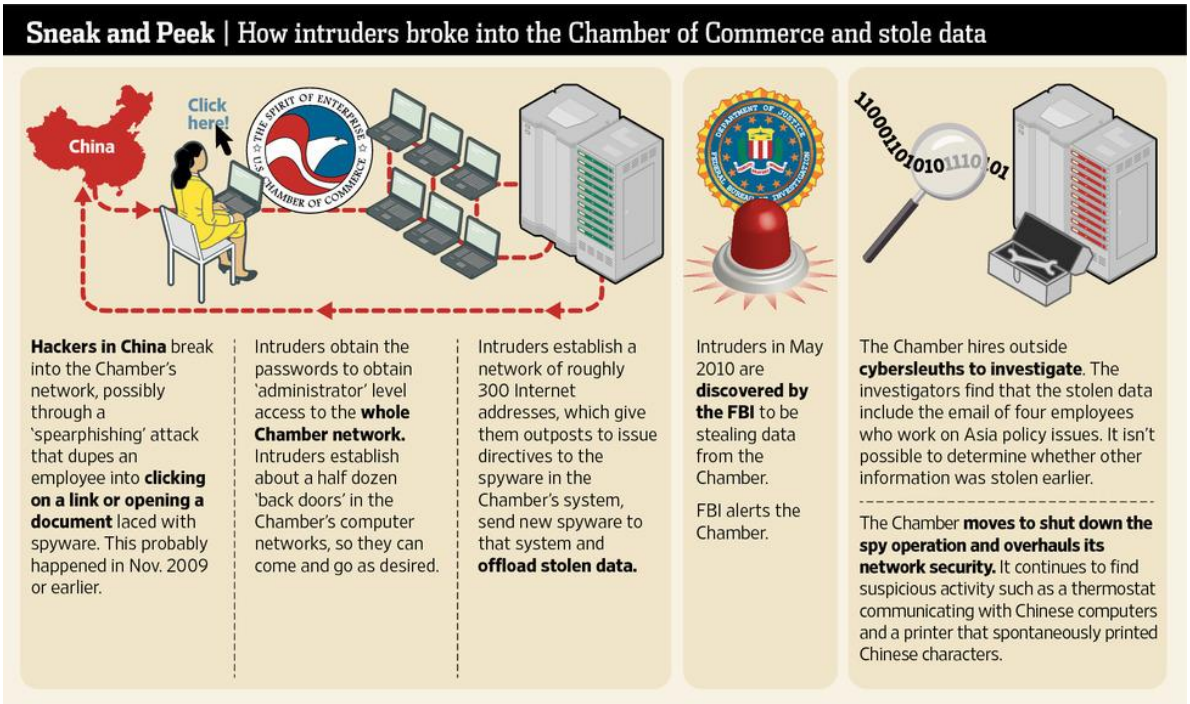
(U) In a recent blog, the CEO wrote: "While the Cold War may be over, the reality is that our country is under cyber attack on a daily basis by world powers such as Russia and China. The difference being, they are invading our data centers and networks, rather than our shores." He wrote that "whether you are in the camp of going on the offensive or employing a strong defense as a way to defeat cyber attacks, it's hard to argue with the logic of making sure that other countries know that if they are going to take a shot at US interests, they are going to get hit back. And hit back hard."

(U) The Fidelis chief concluded: "I often speak to security analysts and business leaders, and I explain to them that security companies who deal with these types of advanced persistent threats (APTs) are becoming the defense contractors of the future. We have become to the cyber world what the likes of Raytheon and Lockheed Martin were to the aerospace industry throughout the 1980s. Alone, we can't win the war for you. But we can equip you with the best weapons to help fight against the bad guys. And if the past is any indicator, the arms race is just beginning to heat up."

(U) China Hackers Hit US Chamber of Commerce (*The Wall Street Journal, 21 DEC 2011; Reuters, 21 DEC 2011*)

(U) A group of hackers in China breached the computer defenses of America's top business-lobbying group and gained access to everything stored on its systems, including information about its three million members, according to several people familiar with the matter. The break-in at the US Chamber of

Commerce is one of the boldest known infiltrations in what has become a regular confrontation between US companies and Chinese hackers. The complex operation, which involved at least 300 Internet addresses, was discovered and quietly shut down in May 2010.



(U) It isn't clear how much of the compromised data was viewed by the hackers. Chamber officials say internal investigators found evidence that hackers had focused on four Chamber employees who worked on Asia policy, and that six weeks of their email had been stolen. It is possible the hackers had access to the network for more than a year before the breach was uncovered, according to two people familiar with the Chamber's internal investigation. One of these people said the group behind the break-in is one that US officials suspect of having ties to the Chinese government. The Chamber learned of the break-in when the Federal Bureau of Investigation told the group that servers in China were stealing its information, this person said. The FBI declined to comment on the matter.

(U) A spokesman for the Chinese Embassy in Washington, Geng Shuang, said cyberattacks are prohibited by Chinese law and China itself is a victim of attacks. He said the allegation that the attack against the Chamber originated in China "lacks proof and evidence and is irresponsible," adding that the hacking issue shouldn't be "politicized." In Beijing, Foreign Ministry spokesman Liu Weimin said at a daily briefing that he hadn't heard about the matter, though he repeated that Chinese law forbids hacker attacks. He added that China wants to cooperate more with the international community to prevent hacker attacks.

(U) The Chamber moved to shut down the hacking operation by unplugging and destroying some computers and overhauling its security system. The security revamp was timed for a 36-hour period over one weekend when the hackers, who kept regular working hours, were expected to be off duty.

(U) Damage from data theft is often difficult to assess.

(U) People familiar with the Chamber investigation said it has been hard to determine what was taken before the incursion was discovered, or whether cyberspies used information gleaned from the Chamber to send booby-trapped emails to its members to gain a foothold in their computers, too. Chamber officials

said they scoured email known to be purloined and determined that communications with fewer than 50 of its members were compromised. They notified those members. People familiar with the investigation said the emails revealed the names of companies and key people in contact with the Chamber, as well as trade-policy documents, meeting notes, trip reports and schedules. "What was unusual about it was that this was clearly somebody very sophisticated, who knew exactly who we are and who targeted specific people and used sophisticated tools to try to gather intelligence," said the Chamber's Chief Operating Officer. Nevertheless, Chamber officials said they haven't seen evidence of harm to the organization or its members.

(U) The Chamber, which has 450 employees and represents the interests of US companies in Washington, might look like a juicy target to hackers. Its members include most of the nation's largest corporations, and the group has more than 100 affiliates around the globe. While members are unlikely to share any intellectual property or trade secrets with the group, they sometimes communicate with it about trade and policy.

(U) US intelligence officials and lawmakers have become alarmed by the growing number of cyber break-ins with roots in China. Last month, the US counterintelligence chief issued a blunt critique of China's theft of American corporate intellectual property and economic data, calling China "the world's most active and persistent perpetrators of economic espionage" and warning that large-scale industrial espionage threatens US competitiveness and national security. Two people familiar with the Chamber investigation said certain technical aspects of the attack suggested it was carried out by a known group operating out of China. It isn't clear exactly how the hackers broke in to the Chamber's systems. Evidence suggests they were in the network at least from November 2009 to May 2010.

(U) The chief information officer at the Chamber, said federal law enforcement told the group: "This is a different level of intrusion" than most hacking. "This is much more sophisticated." The Chamber President and Chief Executive first learned of the breach in May 2010 after he returned from a business trip to China. Chamber officials tapped their contacts in government for recommendations for private computer investigators, then hired a team to diagnose the breach and overhaul the Chamber's defenses.

(U) They first watched the hackers in action to assess the operation. The intruders, in what appeared to be an effort to ensure continued access to the Chamber's systems, had built at least a half-dozen so-called back doors that allowed them to come and go as they pleased, one person familiar with the investigation said. They also built in mechanisms that would quietly communicate with computers in China every week or two, this person said. **The intruders used tools that allowed them to search for key words across a range of documents on the Chamber's network, including searches for financial and budget information, according to the person familiar with the investigation. The investigation didn't determine whether the hackers had taken the documents turned up in the searches.**

(U) When sophisticated cyberspies have access to a network for many months, they often take measures to cover their tracks and to conceal what they have stolen. **To beef up security, the Chamber installed more sophisticated detection equipment and barred employees from taking the portable devices they use every day to certain countries, including China, where the risk of infiltration is considered high. Instead, Chamber employees are issued different equipment before their trips—equipment that is checked thoroughly upon their return.**

(U) Chamber officials say they haven't been able to keep intruders completely out of their system, but now can detect and isolate attacks quickly. The Chamber continues to see suspicious activity, they say. A thermostat at a town house the Chamber owns on Capitol Hill at one point was communicating with an Internet address in China, they say, and, in March, a printer used by Chamber executives spontaneously started printing pages with Chinese characters. "It's nearly impossible to keep people out. The best thing

you can do is have something that tells you when they get in," said the chief operating officer. "It's the new normal. I expect this to continue for the foreseeable future. I expect to be surprised again."

(U) In Beijing, China dismissed the report. Chinese Foreign Ministry spokesman Liu Weimin dismissed the report. "There's nothing to be said about the baseless whipping up of so-called hacking and it won't come to anything," he told a daily news briefing in Beijing. "Chinese law bans hacking."

(U) Analyst Comment: This article notes that the Chamber of Commerce takes to ensure that employees that travel overseas take steps to protect sensitive information. All companies in New Jersey that have employees traveling to foreign countries should take similar steps.

(U) Security Tips from a Legendary Hacker (*CBS News, 19 DEC 2011*)

(U) Kevin Mitnick was once the "most wanted" computer hacker in the world. After being nabbed by the FBI and doing his time, Mitnick became one of the good guys, helping businesses understand and address information security weaknesses and threats. Mitnick, now a leading consultant and speaker on the subject of information security, and author of the New York Times best-seller Ghost in The Wires, spoke with CBS News about the most serious threats of which every business should be aware. Mitnick says that these issues aren't just concerns for large corporations -- small companies face the same challenges, and dealing with them effectively doesn't require massive resources or IT departments.

(U) Here are the top threats, and some tools small businesses can use to address them:

(U) Attacks are becoming more complex

(U) The threat: Attackers have become more sophisticated, and it's often extremely difficult to detect an intrusion until after the damage is done. "Hacker gangs," often operating overseas, have acquired online banking credentials and wired funds out of corporate accounts, or stolen intellectual property, with little or no detection.

(U) The solution: There are several solutions on the market for small- and medium-sized businesses. Cisco (CSCO) and others offer integrated services routers (ISR), which integrate routing, firewalling, intrusion detection, VoIP solutions and wireless networking, at a low cost (entry level models run around $1,000). There are more robust systems for larger enterprises, but ISR provides good baseline protection for smaller businesses.

(U) The risk landscape is increasingly difficult to understand

(U) The threat: Attacks are evolving every day, making it crucial -- and difficult -- to keep up with current hacker methodologies. As a result, thousands of systems are compromised every week. We often hear about distributed denial-of-service (DDoS) attacks carried out by "botnets" of compromised computers. Hackers use similar techniques to gain access to small business computers, where they can access financial and other information, perpetrate theft and do all kinds of other damage.

(U) The solution: Small businesses are increasingly putting many of their system functions in "the Cloud," where they can be kept up-to-date in real time. In these situations, it is critical to clearly outline expectations regarding application and data security in the Service Level Agreement (SLA). If the necessary technical expertise is not available in-house, enlist the services of a security consultant or

qualified IT specialist. Companies like Mitnick's offer advisory services and implementation of the best practices and solutions for keeping up-to-date on threats. For many companies, a modest investment in this kind of expertise can save them from far more costly problems down the road.

(U) Outgoing network traffic can be as dangerous as inbound

(U) The threat: Most businesses have some type of firewall for incoming traffic, but few address potentially risky outgoing connections from their own workstations. This is a major shortcoming, because a user's computer may become infected with malware that connects back to the attacker. According to Mitnick, antivirus software is only 60 percent effective at detecting and eliminating malicious code.

(U) The solution: Reduce the number of services a user can connect to outside the company by configuring the firewall to restrict outgoing traffic to what's necessary for business operations. The ISR solutions mentioned above facilitate this type of configuration.

(U) Desktop software is often out of date

(U) The threat: Hackers used to focus solely on exploiting security flaws at the server level, but this has changed, and individual desktops are now common targets. One of the reasons this is appealing to hackers is that businesses rarely update the client application software that resides on individual workstations. Small businesses can be particularly easy marks for these kinds of attacks.

(U) The solution: Products like Secunia's Corporate Software Inspector automate software updates on user desktops. These updates are as important as applying software and security patches for the operating system, as out-of date software significantly increases the risk of a security breach. Products like the Secunia application can cost a couple-thousand dollars, but again, the investment has to be weighed against the risk.

(U) Humans can be the biggest problem

(U) The threat: The biggest risks to information security are people. Studies have shown that most security incidents start from within, and are usually accidental. Sophisticated attacks use "social engineering" (predicting or manipulating human behavior) to trigger the exploitation of desktop application security flaws.

(U) The solution: Constantly reinforce to employees the dangers of opening attachments and clicking links sent in email, messenger applications and posts on social networking sites. All it takes is one person making a bad decision to compromise the entire business. One clever and effective strategy for keeping employees on their toes is simulating attacks (similar to a surprise military drill), using an Internet Security Awareness Training program, which costs about $15 per person per year.

(U) Of course, these are just quick snapshots of key threats and tools. It's a big and complex subject (Mitnick has filled three books on it so far), but these are great starting steps for most small companies. As Mitnick says, "The most important point is that computer and information security is not, and can never be, a one-size-fits all solution."

(U) As Cyberattacks Grow, Take Security Seriously (*Network World; 29 NOV 2011*)

(U) No company wants to be the subject of the next headline about a cybersecurity attack or critical data loss. Losing business data or customer information takes a toll on your business' reputation and its pocketbook. While it is impossible to entirely avoid an attack, there are steps you can take to mitigate the effects. Ignoring cybersecurity threats and hoping your company isn't a target is not a good strategy. When an organization experiences a cybersecurity attack, it will incur costs, which organizations need to anticipate even before an attack happens. This calls for framing your cybersecurity strategy from a risk management perspective.

(U) The best cybersecurity plan takes into account that no one tactical item will stop a cybersecurity attack. Instead, the plan must take a calculated, serious approach to mitigating cybersecurity attacks once they happen. The next step is to empower the data owners in your business by building in accountability for data security and setting up best practices to secure it. Also, create a budget and priorities for securing data. Make security a part of the organization's culture and make security a theme in all IT policies.

(U) Do you know where your data is? Once your business has adopted a formal cybersecurity plan, you must identify the most critical data to your business:

(U) - Ask what data can your business not operate without. If your company lost client contact information how would it operate?

(U) - What data would harm your business if it were attacked or compromised? Does your business have trade secrets that could be compromised?

(U) - What data would harm your customers if it were attacked? If your business lost sensitive data, such as customers' social security numbers or credit card information, how would it harm your business as well as the customer?

(U) - What business processes does your critical data support? If your business lost its email database contact list, could your sales office still operate?

(U) Once you classify your critical data, determine where the critical data resides and who can access it. To accomplish this, use visualizing applications to determine which users access critical data, where they access it from (i.e. remote access, or via the cloud), and which applications they are using to access it.

(U) Next, prioritize and understand where the risks are within your data. If you make the investment to protect it now, your organization will be in better shape than waiting until after a cybersecurity threat occurs. Reacting under pressure to a threat and playing catch-up means you have lost the upper hand, most likely increasing both the cost of securing your data and the risk of additional threats from suboptimal solutions or prolonged exposure.

(U) Finally, consider implementing a next-generation firewall to monitor and protect your critical data. Next-generation firewalls are a good solution for any size organization and allow you to control and see how applications are being used on your network.

(U) Top Five Security Predictions for 2012 (*20 DEC 2011, PC Magazine*)

(U) Looking back at the headlines of 2011, Security Watch saw some pretty alarming developments this year. Perhaps biggest of all was when the source codes for Zeus and SpyEye botnets were leaked, allowing any punk to easily replicate and spread the malware. Then Anonymous and an emergent group of hacktivists, Lulzsec, disrupted operations of major state and commercial institutions, including the FBI, San Francisco's BART trains, and the Arizona police department. Sony and RSA, a security firm for defense giant Lockheed Martin, suffered devastating data breaches that have squandered millions of dollars so far. And in mobile security, Android malware quadrupled, albeit from a small base.

(U) Looking ahead, what headlines will Security Watch see in 2012? Dozens of security vendors weighed in with their predictions (my personal favorite being: more security vendor predictions). There was very little overlap but below, we name the five most common ones:

(U) 1. First Android worm

(U) A worm is a type of malware that can automatically, and quickly, reproduce itself from one computer to another. We haven't seen them on Android, which explains why less than 5 percent of users in the world have been affected, but Lookout and Fortinet both predict 2012 to be the year of the first Android worm. "Malware writers have had a lot of success infecting users with repackaged versions of applications. Because this is a game of numbers we expect to see malware writers develop tools that enable them to automatically repackage apps with malware and upload them to the market," Lookout wrote in a blog post.

(U) This is dire news for those of you who still think Android malware is pure F.U.D. Back in November, Lookout CTO said that the day we see our first Android worm is the tipping point (or as he called it, the "oh crap" moment) for the propagation of Android malware. Fortinet says the threat will probably come from poisoned SMS messages containing a link to an infected site, or through infected links on Facebook and Twitter.

(U) 2. Your personal data will get stolen from a social network.

(U) This year we saw numerous Facebook and Twitter scams spread through poisoned links to topical subjects, like the deaths of Osama Bin Laden and Amy Winehouse. These scams will only become more sophisticated next year, say many vendors."It is very easy for cyber-criminals to trick users with generic messages like 'Look, you're on this video,' for example. Sometimes, curiosity can be our own worst enemy," said the technical director of PandaLabs.

(U) "Despite improvements in security measures by the social media companies, this concentration of users and data in just a few platforms is irresistible for cybercriminals, so expect more nefarious social media tricks to appear," M86 wrote in its threat predictions white paper. And now that Facebook is moving everyone to frictionless sharing through Facebook Timeline, and on track to hitting 1 billion users next year, cybercriminals will undoubtedly try to thwart Facebook's security measures.

(U) 3. Political Theater

(U) As we gear up for the US general elections later this year, expect to see more politically-focused cyber threats. Predicting an Anonymous attack isn't too far in the left field; we just saw a YouTube video, allegedly from Anonymous, encouraging people to disrupt January's Iowa caucus. Websense, an Internet filtering company, also warned users about searching for next year's big news: the US elections, Mayan calendar, and London Olympics. "Cybercriminals will continue to take advantage of today's 24-hour, up-

to-the minute news cycle, only now they will infect users where they are less suspicious: sites designed to look like legitimate news services, Twitter feeds, Facebook posts/emails, LinkedIn updates, YouTube video comments, and forum conversations," Websense researchers wrote.

(U) Kaspersky Labs predicts that hacktivism, or hacker attacks as a form of protest, will become more political and sophisticated next year. "This will be a more serious trend than in 2011 when most attacks targeted corporations or were carried out just for lulz," Kaspersky wrote. The Russian company also expects to see more state-sponsored attacks as cyberwarfare ramps up.

(U) 4. SMBs Are No Longer Immune

(U) Traditionally cybercriminals target the biggest, most lucrative commercial and state organizations, but next year they're eyeing lower-hanging fruit. According to Kroll, a risk consulting firm, data thieves are "simply looking for the path of least resistance" and lately, that path is in smaller cloud storage providers who can't afford top-notch security like major enterprises. "In addition, ongoing use of legacy systems, weakened by postponed or overlooked upgrades and replacements, put SMBs at heightened risk," Kroll wrote.

(U) PandaLabs had similar thoughts. "Financial institutions are fairly well protected these days against malware. But smaller businesses are easier and cheaper targets to attack, and their customer databases can be a real treasure trove for hackers," PandaLabs noted in its threat predictions. "Unfortunately, many small to medium-sized companies do not have dedicated security teams, which makes them much more vulnerable."

(U) 5. Mac Malware Will Continue to Rise

(U) The phrase "Mac malware," like Android malware, usually elicits a few eyeball rolls. It has evolved so slowly and its sample size is so puny compared to PCs, that most people don't bother using any sort of AV software. But this year we saw a couple persistent pieces of Mac malware, like the fake antivirus program MAC Defender and the CPU-draining Trojan nicknamed 'DevilRobber.' Sophos' Graham Cluely urged Mac users to finally "take Mac malware more seriously." Likewise, McAfee says that as the market share of Mac users continue to grow, so will the number and types of threats we see next year. Read about Mac AV options at Antivirus for Mac: It's Time.

(U) Biggest Security Threat For 2012? Privacy Violations (*Net-Security, 16 DEC 2011)*

(U) Cyber-espionage, along with privacy violations and social networking attacks facilitated by the increased use of mobile and tablet devices, will be the source of increased security threats over the coming months, according to PandaLabs. Cyber-espionage targeting companies and government agencies around the world will dominate corporate and national information security landscapes, with the integrity of classified and other protected information on the line. Trojans are expected to be the weapon of choice for hackers focused on these highly-sensitive targets.

(U) According to the technical director of PandaLabs, "We live in a world where all information is in digital form and is easily accessible if you know how. Today's spies no longer need to infiltrate a building to steal information. As long as they have the necessary computer skills, they can wreak havoc and access even the best-kept secrets of organizations without ever leaving their homes." Consumers will continue to be targeted by cyber-criminals as they find ever more sophisticated ways to target social media sites for stealing personal data. Social engineering techniques exploiting users' naivete have become the weapon of choice for hackers targeting personally-identifiable information.

(U) "Social networking sites provide a space where users feel safe as they interact with friends and family. The problem is that attackers are creating malware that takes advantage of that false sense of security to spread their creations," says the PandaLabs technical director. "It is very easy for cyber-criminals to trick users with generic messages like 'Look, you're on this video,' for example. Sometimes, curiosity can be our own worst enemy."

(U) Following is a summary of what PandaLabs predicts as the major security trends of 2012:

(U) Mobile malware: A year ago, PandaLabs predicted a surge in cyber attacks on mobile phones, and the fact that Android has become the number one mobile target for cyber-crooks in 2011 confirms that prediction. That trend will continue in 2012, with a new focus on mobile payment methods using Near-Field Communications (NFC) as these applications become increasingly popular.

(U) Malware for tablets: Since tablets share the same operating system as smartphones, they are likely be targeted by the same malware. In addition, tablets might draw a special interest from cyber-crooks since people are using them for an increasing number of activities and are more likely to store sensitive data. Mac malware: As the market share of Mac users continues to grow, the number of threats will grow as well. Fortunately, Mac users are now more aware that they are not immune to malware attacks and are increasingly using antivirus programs to protect themselves. The number of malware specimens for Mac will continue to grow in 2012, although still at a slower rate than for PCs.

(U) PC malware: PC malware has grown exponentially over the past few years, and everything indicates that the trend will continue in 2012. Trojans, designed to sit silently on users' computers, stealing information and transmitting it back to their handlers, will continue to be cyber-crooks' weapon of choice; 75 percent of new malware strains in 2011 were Trojans.

(U) SMBs (Small and medium-size businesses) under attack: Financial institutions are fairly well protected these days against malware. But smaller businesses are easier and cheaper targets to attack, and their customer databases can be a real treasure trove for hackers, particularly if credit card and other financial data is stored "in the clear." Unfortunately, many small to medium-sized companies do not have dedicated security teams, which makes them much more vulnerable.

(U) Windows 8: While not scheduled until November 2012, the anticipated next version of Microsoft's operating system will offer cyber-crooks new opportunities to create malicious software. Windows 8 will allow users to develop malware applications for virtually any device (PCs, tablets and smartphones) running this platform, although this will likely not take place until 2013.

(U) Small Firms Have Fewer Resources to Deal with More Cyberthreats, House Panel Told (*InfoSecurity Magazine, 05 December 2011*)

(U) A majority of cyberattacks target small businesses, yet they have fewer resources than larger firms to combat these threats, a House panel was told in early December. “Although we often hear about cyber attacks on large businesses and institutions, a recent report shows the majority of these attacks are on small firms. Small businesses generally have fewer resources available to monitor and combat cyber threats, making them easy targets for expert criminals”, said Rep. Renee Ellmers (R-N.C.), chairwoman of the House Committee on Small Business subcommittee on healthcare and technology.

(U) Ellmers' panel examined the issue of small business and cybersecurity at a hearing held last week. Among those testifying was Michael Kaiser, executive director of the National Cyber Security Alliance (NCSA). Kaiser told the panel that his organization conducted a survey of 1,045 small businesses in October with Symantec and Zogby. The survey found that 59 percent of small businesses did not require any multifactor authentication for access to their networks, 67 percent allowed the use of USB devices in the workplace, and 50% did not completely wipe data from their machines before disposal.

(U) In addition, 77 percent of respondents did not have a formal written Internet security policy for employees; of those who did not have a formal policy, almost half did not have an informal policy either. A majority of respondents (56 percent) did not have Internet usage polices that clarify what websites and web services employees could use. Almost two-thirds (63 percent) did not have policies regarding how their employees use social media; 40 percent did not have a privacy policy in place that their employees must comply with when they handle customer information; and almost half did not have a plan or strategic approach in place for keeping their business cyber secure. Yet, cybersecurity is increasingly important to the value of the business, according to the survey. Seven in ten said that Internet security is critical to their business success, and 57 percent said that having a strong cybersecurity posture is good for their brand.

(U) Tips for IT Security, at Home and On the Road (*PC Magazine, 20 DEC 2011*)

(U) Staying connected is a necessity of modern life; the problem comes when you accidentally make a hazardous connection. Any time you're on the Internet or using your smartphone, you might conceivably be picking up malware, or losing personal information to a hacker. But don't go overboard; full-scale paranoia is not required. There's no need to smash all your devices and put on a tinfoil hat. Yes, there are so many steps you can take to protect yourself that remembering them all may seem overwhelming. The important thing is to focus on what's most important for your current situation. Here are tips for a variety of locations, at home and away.

(U) Traveling light, with no devices

(U) • Don't log in to secure sites on unsecured kiosks or public computers
(U) • Clear recent history (Ctrl+Shift+D in IE, Firefox, or Chrome) after using any computer that isn't yours
(U) • If you need secure access, use a VPN client
(U) • Beware the hotel room phone–charges may be through the roof

(U) Traveling with a smartphone

(U) • Don't log in to secure sites while connected through unsecured wireless
(U) • Be almost as cautious when connected through password-protected wireless
(U) • Check with your carrier if going overseas; you may need to enable international roaming
(U) • Beware insanely high charges for data roaming in other countries
(U) • Secure your smartphone with a strong password, not just the default 4-digit PIN
(U) • Consider installing a mobile security app that can remotely lock and wipe the phone and also locate if it's lost or stolen

(U) Traveling with a laptop

(U) • Never leave the laptop in sleep mode, where a thief could simply "wake it up" and have full access. Either shut it down or put all the way into hibernate

(U) • Make sure the laptop is configured to require a password on coming out of hibernate
(U) • If you're carrying truly sensitive data, consider using Windows's BitLocker Whole Disk Encryption or a third-party encryption tool
(U) • Consider installing a laptop antitheft tool that can lock down the laptop and trace the thief

(U) At Home

(U) • Change your router administrator password to something other than the default. There are websites that list the defaults for virtually all models
(U) • Use a password manager to generate and protect strong passwords—you can store your router password here too
(U) • If you have a wireless network, be sure to change the SSID to something other than the default, and encrypt the connection
(U) • Install antivirus protection, if you don't already have it, or better yet a full security suite

(U) At Work

(U) • Don't go to lunch or on a break without locking your desktop. This prevents co-workers from snooping or playing tricks
(U) • Don't log in to secure sites for personal business. Remember, the company owns that computer, and the network, and the network logs. Assume anything you do on the company computer is public
(U) • If you're steamed about something, calm down before emailing. Check to make sure your tone is civil, and be very sure you don't Reply All when it isn't appropriate
(U) • Find out if your company has policies in place about security; if so, learn and heed them

(U) Be sure to keep your brain engaged and your common sense active. That notification from your bank about a credit problem might be bogus, so navigate to the bank site yourself rather than clicking any links. And just as in the non-Internet world, if you come across an offer that seems too good to be true, it's probably a scam. If you focus on the right safety tips, you can protect yourself, your data, and your identity no matter where you are.

(U) FBI Warns Hacktivists: You're Breaking the Law (*CIO Magazine, 19 DEC 2011*)

(U) Last July, the FBI executed what is arguably its most public campaign against hacktivists, individuals who breach computer systems to make a political or ideological statement. On Tuesday, July 19, the G-men cuffed 12 men and two women allegedly associated with hacktivist group Anonymous for their supposed involvement in a dedicated denial of service (DDoS) attack against PayPal's website in December 2010.

(U) The July raid appeared to be the largest public indication that the FBI was finally making headway in its investigation of hacktivist activity during a year when groups including Anonymous and LulzSec made a mockery of public- and private-sector computer systems. Between December 2010 and August 2011 alone, they broke into dozens of corporate and government networks with outrage, defiance and glee. In fact, hacktivist activity had long been on the FBI's radar, according to Shawn Henry, executive assistant director of the FBI's Criminal, Cyber, Response and Services Branch. He first noticed it in the late 1990s, when he was working as a supervisory special agent at FBI headquarters on computer intrusion cases. At the time, hacktivism consisted mostly of website defacements, he says. Today, it's more menacing.

(U) Consider the outcomes of just three data breaches launched in the name of hacktivism:

- (U) LulzSec's hack into Sony's PlayStation network in April 2011 is reportedly expected to cost Sony $171 million by the end of the entertainment company's 2012 fiscal year.

- (U) When Former HBGary Federal CEO Aaron Barr threatened to expose top members of Anonymous, the hacktivist group retaliated by breaking into the security company's systems and exposing controversial and confidential emails. Barr subsequently received death threats and was forced to step down from his job.

- (U) After Anonymous broke into the member database for Bill O'Reilly's website, a woman who's name, email address, physical address and password were exposed during the breach suffered $400 in fraudulent credit card charges and huge amounts of embarrassment after hackers posted pornographic pictures to her Facebook page and sent pornographic emails via her AOL account, according to Ars Technica.

(U) Henry maintains that the FBI isn't motivated by hacktivist groups' ideological agendas. What matters most to the FBI, he says, is that these groups are breaking the law. "When anybody breaches a network and steals data and then publicizes it—whether they're from a foreign country and they're using the data to help their country's industry, they sell it as an organized crime group, or they just display it because they think the company they stole it from is acting inappropriately—the fact that the data is stolen is a violation of federal law," he says, his voice rising with conviction. "Hacktivism is no different from organized crime groups or foreign governments. It's the exact same activity, perhaps done for a different reason or purpose, and it's all still illegal."

(U) In this exclusive interview with CIO.com, Henry speaks for the first time with the media specifically about hacktivism. Though Department of Justice guidelines prevented him from discussing specific hacktivist groups and open cases, he describes the threat hacktivists pose, the challenges associated with investigating them, and the FBI's success disrupting these groups. He also has a special message for hacktivists.

(U) CIO.com: What threat do hacktivists pose? Is there some threat that their ideology poses, in addition to breaking into computer systems?

(U) Shawn Henry: I look at three different threats to our critical infrastructure in the United States:

- (U) [The first is] organized crime groups that primarily access the networks of the financial services sector. They steal data and monetize it to the tune of hundreds of millions of dollars a year.

- (U) There are foreign governments breaking into computer networks and stealing data from .mil, .gov and .com domain names. They steal data to help their governments compete with the United States, to help their industry. That's being done to the tune of billions of dollars a year.

- (U) Then there are individual hackers breaking into networks for other reasons. It may be for personal interest—hacking computers to test their skills. They may be hacking into computers to make some type of a statement.

(U) All of those groups—regardless of whether they're organized crime operating out of Eastern Europe, a foreign government, or a 16-year-old kid down the block—once they're in, they have gained control of

that network. They have the ability to do a lot more than steal data. They have the ability to change data. So data integrity is at risk. They have the ability to turn off data. They can shut the network down if they gain administrative access. If I'm the owner of a network, it doesn't matter who's in my "house": If each and every one of those groups has the ability to do the exact same thing, I'm at significant risk. Anybody who has that administrative access to that network has the ability to steal data, change data and deny us access to our own data.

(U) CIO.com: What makes investigating these organizations and individuals so difficult?

(U) Henry: One of the most significant challenges is attribution: How do you identify who committed the crime? In the physical world, if someone robs a bank, we have video cameras and maybe eye witnesses. We may have evidence, fingerprints. We have clues right away. The pool of subjects who may have robbed that bank is limited to the number of people in the vicinity of the bank at the time of the robbery.

(U) In the cyber world, the pool of candidates is limited to anybody who has access to an Internet connection at any time in the world, regardless of where they're sitting. That increases the pool of candidates. [Moreover,] the evidence we have is digital. It's fragile. It's transient. Regardless of who the actor is, intrusion investigations by nature are complex. They're most often international in nature—they have some international nexus—whether beginning or ending overseas. There are advantages to working these cases. The biggest advantage for us is the partnerships we've developed internationally. Many countries around the world recognize that this is a worldwide problem. We've had a lot of success working with our partners internationally.

(U) CIO.com: How can you say the FBI has been successful when a hacker claiming to be affiliated with Anonymous recently launched a successful attack on CLEAR (Coalition of Law Enforcement and Retail) that resulted in the exposure of the names, phone numbers, email and home addresses, and passwords of more than 2,400 law-enforcement, federal, military, loss-prevention and corporate professionals? And last month, Anonymous and TeaMp0isoN announced a new attack on major banks.

(U) Henry: We've had success in the United States against cancer, but thousands of people die from cancer every year. We've had success in organized crime. There's still organized crime in this country, but we've arrested thousands of people involved in organized crime over the years and put heads of organized crime in prison.

(U) To say we haven't been successful because we see activity, you have to look at the totality. We have been successful in this area. There are some statistics that have been published on the number of arrests we've made. It's not near the totality of our success in this year. We've identified people. We've arrested people in intrusion cases—in many cases, people who have impacted major networks, people who have stolen millions of pieces of data, people who have been responsible for tens of millions or hundreds of millions of dollars in damages in the United States. A lot of our successes aren't publicized for operational purposes.

(U) Final Thoughts From Henry to Hacktivists

(U) "The FBI is a believer in civil rights and civil liberties, and the first amendment is something I hold very dear personally and professionally. I have no problem with people picketing and protesting in the street. I get all that. But the freedom for me to swing my arm ends where your nose begins. If you are impinging on others' rights, that's illegal. "I encourage people to promote and express their views. We in this country have probably the most robust system to enable that. We have laws that allow people to express their views. We have so many freedoms in that area that people who violate the law are way

outside their lane. There are so many opportunities for people to do it lawfully that it's irresponsible for them to do it otherwise."

(U) Bill Would Allow US intelligence to Share Cyber-Threat Info; Legislation Would Help Protect US Businesses Against Cyberattackers, Sponsors Say (*IDG News Service, 30 NOV 2011*)

(U) A new bill introduced by senior members of the US House of Representatives Intelligence Committee would allow intelligence agencies to share classified cyber-threat information with approved US companies, while encouraging companies to share their own information. The Cyber Intelligence Sharing and Protection Act, introduced in November, is a "significant first step" toward protecting the US government and businesses from constant cyberattackers, said Representative Mike Rogers, a Michigan Republican and committee chairman. "There is a cyberwar that is going on today," Rogers said during an event to announce the bill.

(U) The bill would direct the US director of national intelligence to set up a process for intelligence agencies to share cyber-threat information and for granting security clearances at organizations that want to receive the information. Businesses that receive the classified information would generally be limited in their use of the information to protecting themselves or their customers. The bill would also give lawsuit protection to companies that use the information to protect their networks or share cyber-threat information. The bill would allow companies to share cyber-threat information anonymously through an undefined process or restrict who they share with, including the government. "If we're going to win this fight, we have to have more sentries on guard," Rogers said. "What this bill will do is leverage every private IT security operation in every company in America to be on guard."

(U) The bill does not require companies to share any information and includes no new mandates for businesses, Rogers said. "These companies are under assault every single day," he said. "It is in their best interest to cooperate." Without improved cybersecurity the United States will have a "catastrophic" cyberattack within the next year, predicted cosponsoring Representative C.A. "Dutch" Ruppersberger of Maryland, the senior Democrat on the committee. "We simply can't stand by if we have the ability to help American companies protect themselves," he said. "Sharing information about cyber-threats is a critical step to preventing them."

(U) Trade groups the Information Technology Industry Council and the National Cable and Telecommunications Association (NCTA) were among the organizations voicing support for the bill. The cyber-threats facing US businesses are "deeply frightening," and the bill will improve national security, said Michael Powell, NCTA's president and CEO.

(U) COUNTERTERRORISM THREAT ITEMS FROM THE PRESS:

(U) DHS Director Napolitano: Lone Wolf Terror Threat Growing (*The Associated Press, 02 DEC 2011*)

(U) US Homeland Security Director Janet Napolitano said in December that the risk of "lone wolf" attackers, with no ties to known extremist networks or grand conspiracies, is on the rise as the global terrorist threat has shifted. Such risks, Napolitano said in an interview in Paris, heighten the need to keep dangerous travelers from reaching the United States, and she urged European partners to finalize a deal on sharing passenger data that has met resistance over privacy concerns. Napolitano acknowledged shifts in the terror threat this year, but said the changes had little to do with the uprisings that have overturned the old order in countries around the Arab world and opened up new opportunities for extremist groups.

(U) Asked about the greatest current threats to the United States, she said one from al Qaeda has morphed. "From a US perspective, over the last several years we have had more attacks emanating from AQAP (al Qaeda in the Arabian Peninsula) than from core al Qaeda," she told The Associated Press. "There's been a lot of evolution over the past three years," she said. "The thing that's most noticeable to me is the growth of the lone wolf," the single attacker who lives in the United States or elsewhere who is not part of a larger global conspiracy or network, she said.

(U) She named no examples, but it's a phenomenon that is increasingly the focus of international anti-terror operations. A former US Army psychiatrist is the sole suspect in deadly shootings at Fort Hood, Texas, in 2009. In March, a Kosovo Albanian acting alone fatally shot two American airmen in Frankfurt, Germany. In April, a remote-control bomb exploded in a Marrakech cafe popular with tourists, killing 17 people, mostly foreigners, an attack devised by a Moroccan who was inspired by al Qaeda and tried unsuccessfully for years to join the international terror network before returning to Morocco to devise an attack of his own.

(U) One threat that has remained constant, Napolitano stressed, is that of terrorists reaching US territory. She said the agreement with the EU on sharing data on air passengers for flights from Europe to America is needed to "make sure these global networks and global systems that we all rely on remain safe." She stressed that such data aided high-profile US terrorist investigations in recent years, including that into Najibullah Zazi, who admitted plotting to bomb New York subways, and David Headley, who was involved in the 2008 Mumbai, India, terrorist attack.

(U) Man Pleads Guilty In Plot to Attack Military Recruiting Station in Seattle (*The Seattle Times, 08 DEC 2011; The Washington Post, Associated Press; 07 DEC 2011*)

(U) One of two men accused of planning to attack a Seattle military recruiting station last summer pled guilty to federal charges that include conspiracy to use weapons of mass destruction. Walli Mujahidh faces up to 32 years in prison for the plea to conspiracy to kill officers of the United States, conspiracy to use weapons of mass destruction and unlawful possession of a firearm. His attorney said Mujahidh, 32, has serious mental health issues. He has been diagnosed with schizoaffective disorder with bipolar tendencies.

(U) Mujahidh and Abu Khalid Abdul-Latif, 33, a felon and a Muslim convert, were arrested June 22. They were named in a nine-count indictment July 7 alleging they conspired to murder officers and employees of the US government, conspiracy to use a weapon of mass destruction (a grenade) and possession of a firearm in furtherance of a crime of violence. Those charges carry potential life sentences, and the firearm charge includes a mandatory-minimum 30-year sentence that must be served consecutively to any other sentences. Federal prosecutors say the men were taken into custody when they arrived at a warehouse garage to pick up machine guns to use in the attack. **The alleged target, the Military Entrance Processing Station (MEPS) on East Marginal Way in Seattle, was a recruiting station for all military branches. The pair initially planned an attack on Joint Base Lewis-McChord, but later shifted to what they considered an easier target, the complaint said.** According to court documents and law-enforcement sources, he had initially chosen Joint Base Lewis-McChord as a target at least partly because Stryker soldiers there are being court-martialed for allegedly murdering Afghan civilians.

(U) Investigators say they learned of the plot when someone that Abdul-Latif recruited to obtain weapons turned to Seattle police and then acted as a paid confidential informant. Abdul-Latif is also known as Joseph Anthony Davis, and Walli Mujahidh is also known as Frederick Domingue Jr. Authorities say they

were inspired in part by the massacre at Fort Hood, Texas, and the recent prosecutions of Washington state-based soldiers for the deaths of three Afghan civilians. They planned the attack for weeks and fantasized about the media attention they'd receive, according to a federal complaint. Abdul-Latif was scheduled to face trial next May.

(U) Prosecutors did not divulge how the suspects became acquainted, though Mujahidh formerly lived in Seattle. He was convicted in municipal court of violating a domestic violence protection order stemming from a 2007 incident. Mujahidh voluntarily spoke with investigators after the arrests and confessed, according to the federal complaint against them. Abdul-Latif, 33, has a criminal record and a troubled family past, but allegations that he plotted a terrorist attack surprised those who knew him. He appears to have posted several videos on YouTube expressing sympathy for al-Qaida's leader in Yemen and excitement about a radical interpretation of Islam.

(U) Analyst Comment: This case highlights that individuals planning to conduct violent attacks conducted pre-operational planning and surveillance, and changed the potential target of their attack (from Joint Base Lewis – McChord to a Military Entry Processing Station) to an "easier target". Security officials should be alert to indicators of surveillance and pre-operational planning and also take steps to maintain robust force protection measures.

(U) Tarek Mehanna Guilty of Terror Charges; Massachusetts Man Attempted to Promote, Join War Against United States (20 DEC 2011, The Boston Globe)

(U) Tarek Mehanna, the pharmacy college graduate from the quiet, affluent suburb of Sudbury, MA, was convicted in December of providing material support to Al Qaeda, in a swift and sweeping verdict that found he sought paramilitary training in Yemen so he could carry out jihad, or holy war, against US soldiers in Iraq. Mehanna was convicted on seven charges, and he was also convicted of using his knowledge of Arabic to translate and distribute documents promoting Al Qaeda's ideology, to inspire others to violent jihad. The 29-year-old remained calm and poised as the verdict of guilty was announced repeatedly in US District Court in Boston, a total of seven convictions for counts of conspiring to provide material support to terrorists, conspiring to kill in a foreign country, and of lying to authorities in a terrorism investigation.

(U) Once the jury was discharged, he yelled out, "I love you'' to his crying mother, Souad, to his father, Ahmed, and his younger brother, Tamer, and he thanked dozens of supporters. He is slated to be sentenced on April 12 and faces life in prison. His father would only say: "I'm stunned, I can't believe it.'' Prosecutors said the verdict was just. "The job of law enforcement agencies and prosecutors is to bring terrorists to justice,'' a US Attorney told reporters after the verdict. "And it is vitally important that we prevent incidences of terrorism before they happen.'' Richard DesLauriers, special agent in charge of the FBI's Boston division, said: "The FBI has a clarion mission to investigate all potential threats to the United States in order to protect our community from harm. The FBI fulfilled its most important mission by stopping Mehanna's conspiracy to support terrorism, the goal of which was an unlawful affront to our nation's cherished ideal of peaceful dissent.''

(U) Mehanna continued to receive support from family members, friends, and civil rights groups who said the prosecution for his translation and distribution of documents was an infringement of his rights, as an American citizen, to free speech. Mehanna had argued that he was devoted to his religion and the rights of Muslims to defend themselves, but said he never worked for Al Qaeda. "It's an incredibly sad day for us,'' one of Mehanna's attorneys, said after the verdict was read. ". . . It is a sad day for civil rights. It is a sad day for the First Amendment.'' Another defense attorney said Mehanna will appeal the verdict, in large part on the argument that prosecutors sensationalized the trial by repeatedly referring to and

showing pictures and videos of Osama bin Laden and suicide bombings, as a strategy to scare and prejudice jurors.

(U) The jury of six men and six women deliberated for about 10 hours before rendering its verdict, following 31 days of testimony by more than 40 witnesses in what both sides agree was a complex trial. Several jurors contacted by the Globe refused to comment on their deliberations. Over the course of the trial, FBI agents testified of videos of suicide bombings and of the Sept. 11, 2001, terrorist attacks that were found on Mehanna's computer, following a secret search of his Sudbury home in 2006. Mehanna also possessed videos and documents produced by Al Qaeda, and prosecutors said he used his knowledge of Arabic to translate them, following Al Qaeda's call for followers to spread its message in the West. Prosecutors say the information showed Mehanna's state of mind in 2004, when he traveled to Yemen with a friend, Ahmad Abousamra. A third man, Kareem Abuzahra, joined them but returned halfway through the trip after his father had reportedly gotten ill.

(U) Abuzahra was also investigated, but he cooperated with authorities and testified under immunity that the three of them discussed going to Yemen to seek paramilitary training, so they could fight in Iraq. Abuzahra testified that Mehanna had told him once he returned to the United States that he failed to find a terrorist camp, and he said they agreed to tell investigators a cover story that they went to Yemen in search of schooling. Defense attorneys sought to impeach the testimony of Abuzahra, who was seen as the government's key witness. The lawyers got him to acknowledge that he was the one amongst his friends who inquired about obtaining weapons and who discussed the possibility of a domestic terror attack at an Air Force base or shopping mall.

(U) But Mehanna, the defense team argued, was a budding scholar who dismissed the idea of attacking American civilians or a domestic attack, a philosophy that was at odds with Al Qaeda. They said any views he had were rooted in his devotion to his religion and the belief that Muslims should defend themselves, particularly against foreign soldiers in Iraq. They also argued that Mehanna's views were far more moderate than others, including those of his own friend Abousamra. Abousamra, they agreed, sought training in Iraq, but argued that Mehanna should not be held accountable for his actions. Abousamra was charged, but fled to Syria after he was first questioned in 2006, and he remains a fugitive.

(U) The case against Mehanna stirred much controversy within the greater Muslim community, after Mehanna said he had been threatened by FBI agents with prosecution for failing to cooperate and serve as an informant. Many who never met Mehanna rallied to his cause and attended the two-month trial. Mehanna never fled after he was first contacted by authorities in 2006, his supporters point out. He was not charged until 2008, as he was about to board a flight to Saudi Arabia to begin a career as a pharmacist.

(U) A US Attorney said Mehanna was charged based on his own conduct. "We do not prosecute people for expressing their beliefs, for exercising their freedom of speech and their First Amendment rights,'' she said. "We prosecute people for conduct and the intent that they have when they engage in certain conduct.'' Mohamed Islaam, who described himself as a friend of Mehanna's from New York, walked out of the courthouse convinced Mehanna had been punished for refusing to work as an informant. Islaam also pointed out that Mehanna left the courtroom with the same sense of inner calm that he had when he entered it. "His head was held high,'' he said. "He's an honorable man. He knows he's innocent.''

(U) NY Man Gets Probation for Illegal Money Transfer in Failed Terror Attack on Times Square (*Associated Press, 01 DEC 2011*)

(U) A man unwittingly swept up in a failed terror plot to bomb Times Square last year was sentenced to three years' probation. Mohammad Younis had pleaded guilty to charges he arranged an illegal transfer of $7,000 to Faisal Shazad, money Shazad claimed that the Pakistani Taliban provided to fund his one-man strike against New York City. Younis and his brother in Pakistan were part of underground money transfer system known as hawala, authorities said. When the Times Square attack was in the planning stages, Younis' brother sent him the cash that he delivered to Shazad at a Long Island railroad station.

(U) Prosecutors in federal court in Manhattan acknowledged that Younis never knew about Shazad's plot. But they argued that a potential sentence of up to six months would be appropriate to deter money transmissions that could fund terrorism. Attorneys for the Pakistan-born Younis asked for leniency, describing him as a working-class immigrant who posed no danger. "I'm really sorry," Younis told the judge before he was sentenced. "It will not happen ever, ever again." Shazad is serving a life sentence after admitting he built a car bomb he left in Times Square to avenge US military intervention in Muslim countries. The bomb malfunctioned but still spread fear throughout the city.

(U) San Diego Woman Admits Aiding Terrorists (*NBC San Diego, 01 DEC 2011*)

(U) A San Diego woman has admitted she gave money to a foreign terrorist organization in Somalia and then lied to federal investigators about it. Nima Yusuf, 25, pled guilty in federal court to providing approximately $1,450 to al-Shabaab between February and November 2010. Yusuf also made false statements when she denied sending the money in interviews with an FBI agent and Customs and Border Protection officer.

(U) As part of her guilty plea, Yusuf admitted to working with four men currently accused of supporting the same organization. Mohamed Abdullahi Hassan, Abdisalan Hussein Ali, Cabdulaahi Ahmed Faarax and Abdiweili Yassin Isse are being charged separately under a grand jury indictment in Minnesota. Yusuf (aka Nimco Ali Yusuf, Amina Ahmed and Amina Ali), was the fourth person charged in San Diego with helping al-Shabaab. FBI agents arrested Basaaly Saeed Moalin, 33, of San Diego on Oct. 31, 2010 just before he was about to board a flight at Lindbergh Field. The following day, agents arrested Mohamed Mohamed Mohamud, 38, and Issa Doreh, 54, both of San Diego.

(U) Yusuf's next court appearance is scheduled for Feb. 10, 2012. She remains held without bail pending sentencing. She faces a potential maximum sentence of 15 years in prison and a $250,000 fine. Al-Shabaab is an al-Qaida-linked militia trying to create an Islamic state in Somalia and has used violence and intimidation to further its cause.

(U) Iraqi Pleads Guilty in Kentucky to Trying to Assist Al-Qaida (*The Associated Press, 16 DEC 2011*)

(U) An Iraqi man who had claimed he was innocent of terrorism-related charges did an abrupt about-face, pleading guilty in a Kentucky courtroom in December to trying to funnel weapons and cash to al-Qaida operatives in his home country. Waad Ramadan Alwan, 30, appeared in federal court in this south-central Kentucky college town to plead guilty to conspiring to attack American soldiers in Iraq, conspiring to use a weapon of mass destruction and attempting to provide material support to terrorists.

(U) Alwan was arrested in May in Bowling Green and had previously pleaded not guilty to charges in an indictment that also named fellow Iraqi Mohanad Shareef Hammadi. "Today in open court, Waad Alwan admitted to engaging in terrorist activities both here in the United States and in Iraq," a US Attorney said in a statement. "He acknowledged he had built and placed numerous improvised explosive devices (IEDs) aimed at killing and injuring American soldiers in Iraq, and he admitted that he tried to send numerous weapons from Kentucky to Iraq to be used against American soldiers." The US Attorney said the joint efforts of federal and local law enforcement had thwarted "the ongoing intentions of an experienced terrorist." "The guilty plea today sends a strong message to anyone who would attempt similar crimes that they will face the same determined law enforcement and prosecution efforts," he said.

(U) Alwan, appearing in an orange jail jumpsuit and wearing leg irons and with an interpreter seated next to him, pleaded guilty to all 23 counts in the indictment against him. At one point in the proceedings, Alwan nodded and quietly told the interpreter he understood the charges and possible penalties. He faces a possible sentence of 25 years to life in prison when he is sentenced April 3. Alwan pleaded guilty to charges of conspiracy to kill US nationals abroad, conspiracy to use a weapon of mass destruction against US nationals abroad, distributing information on how to make and use improvised explosive devices, attempting to provide material support to terrorists and conspiracy to transfer, possess and export Stinger missiles.

(U) Hammadi, 24, was not mentioned during the hearing, and no trial date has been set for him. He has pleaded not guilty. Hale declined to say whether Alwan would testify against his co-defendant. "We can't discuss that issue," he said. Hammadi's attorney said that Alwan's guilty plea does not affect Hammadi's case. When asked if Hammadi might also plead guilty, Earhart said, "We're continuing to explore that, but we've not reached any agreement."

(U) Before the hearing, Alwan rubbed his eyes occasionally and would sometimes rest his chin against one of his hands. Responding to a litany of questions from a Senior US District Judge, Alwan offered a brief autobiographical sketch, saying he had a high school education and had been a chicken factory worker in the United States. He showed no emotion before the hearing or while answering the questions from the judge. Alwan and Hammadi were living as refugees in Kentucky when they were arrested after an investigation that began months after their arrival in the United Sates in 2009. Neither has been charged with plotting attacks within the United States, and authorities said their weapons and money didn't make it to Iraq because of a tightly controlled undercover investigation.

(U) Alwan was also charged with conspiring to attack American soldiers in Iraq. Other charges include conspiracy to use a weapon of mass destruction and attempting to provide material support to terrorists. Hammadi is also charged with attempting to provide material support to terrorists and conspiring to transfer, possess and export Stinger missiles. Alwan admitted to trying to supply al-Qaida in Iraq with a cache of weapons that included machine guns, rocket-propelled grenade launchers, plastic explosives, sniper rifles, Stinger surface-to-air missile launcher systems and grenades. Authorities have said the weapons and money didn't make it to Iraq because of a tightly controlled undercover investigation.

(U) On multiple occasions, Alwan transferred money believing it would go to al-Qaida in Iraq for the purpose of killing Americans overseas, according to prosecutors. Alwan admitted to trying to feed the cash and weapons pipeline to al-Qaida from September 2010 through May 2011 from Kentucky. While in Iraq, Alwan conspired with others to plant and detonate numerous roadside bombs against US troops, according to the plea agreement and other court documents. Alwan's fingerprints were lifted off an improvised explosive device found in Iraq in 2005. Before he entered the United States as a refugee in 2009, he had to provide a set of fingerprints for a security check. Prosecutors said that from about 2003 through 2006, Alwan conspired to kill US nationals in Iraq. Alwan also drew diagrams of improvised explosive devices and provided detailed oral instructions on how to make and use them, prosecutors said,

adding that the diagrams were intended to train others in how to make and use the bombs in order to kill Americans overseas.

(U) Nigerian Terrorists Pose Threat to United States; House Subcommittee Calls Attention to Rise of Boko Haram (*The Washington Times, 30 NOV 2011*)

(U) The Nigerian Islamist terrorist group Boko Haram poses an "emerging threat" to the United States and is set to join other al Qaeda affiliates in plotting attacks against the US homeland, a congressional panel said in late November. US intelligence agencies must not underestimate Boko Haram's ability and desire to strike directly at the United States, a mistake they made with al Qaeda affiliates in both Pakistan and Yemen in recent years, a House Homeland Security subcommittee said in a bipartisan staff report published at a hearing. "The US intelligence community must not underestimate Boko Haram's intent and capability to strike US interests and most importantly, the US homeland," said Rep. Patrick Meehan, Pennsylvania Republican and chairman of the Homeland Security subcommittee on Counterterrorism and Intelligence.

(U) The report noted that Boko Haram has begun to employ hallmark al Qaeda tactics in oil-rich Nigeria. The terrorists have used truck bombs, coordinated multiple suicide attacks and released martyrdom videos. There have also been increasingly close connections between some Boko Haram leaders and al Qaeda-linked groups in Africa, like al Shabab in Somalia and al Qaeda in the Islamic Maghreb, it said. In August, Boko Haram attacked the U.N. headquarters in the capital Abuja with a suicide truck-bomb, killing 21 people in its first attack against an international target. It has also threatened Nigeria's oil infrastructure. The U.N. attack and reports of links between Boko Haram and other Islamist terror groups "may signal a shift [from a purely national or regional strategy] towards a more global militant ideology," said California Rep. Jackie Speier of California, the senior Democrat on the subcommittee.

(U) The rapid evolution in tactics and targets by Boko Haram "mirrors" the trajectory taken by other al Qaeda affiliates, which have attempted to strike directly at the United States. Mr. Meehan noted that the so-called "underwear bomber" who tried to blow up a United States-bound airliner on Christmas Day 2009 was linked to al Qaeda in the Arabian Peninsula. He added that the failed truck-bombing of Times Square in New York in May 2010 was plotted by a Pakistani-American trained by the al Qaeda-linked Tehrik-i-Taliban Pakistan. "There is little evidence at this moment to suggest that Boko Haram is planning attacks against the homeland," said Mr. Meehan. However, he added, that a "lack of evidence does not mean that it cannot happen."

(U) Mr. Meehan noted that US intelligence agencies have "very recently been wrong about al Qaeda affiliates' intent and capability to strike the homeland with nearly deadly consequences." "We underestimate emerging terror groups at our peril," he said. A well-coordinated series of attacks by Boko Haram in Nigeria could "completely [cut] off oil production in the West African nation and cause a "spike in oil prices worldwide and soaring domestic gas prices," the report warned Nigeria is the world's fourth largest oil producer and accounted for eight percent of US oil imports last year.

(U) Ms. Speier cautioned that little is known about Boko Haram in part because of its "rapid rise." She urged US agencies to redouble their efforts to find out about its "membership strength and leadership cadre," as well as "the true nature of its ties to other groups." She called for increased counter-terrorism cooperation with the Nigerian government and "outreach to the Nigerian people, especially the Muslim community," to help US officials "better understand the appeal of a group like Boko Haram." About half of Nigeria's 155 million people are Muslims and 40 percent of the population is under 40 years old.

(U) NY Prosecutor: Hezbollah Laundered Millions in United States (*Associated Press, 15 DEC 2011*)

(U) Federal authorities blamed Lebanese financial institutions for wiring more than $300 million into the United States in a money-laundering scheme they said used the US financial system to benefit the militant group Hezbollah. The US government said in the lawsuit filed in a Manhattan federal court in December that it seeks nearly a half-billion dollars in money-laundering penalties from some Lebanese financial entities, 30 US car buyers and a US shipping company. It also said it's entitled to claim their assets as forfeitable under US money-laundering laws. Prosecutors said the $300 million was wired from Lebanon to the United States used to buy used cars and ship them to West Africa. They said Hezbollah money-laundering channels were used to ship proceeds from the car sales and narcotics trafficking back to Lebanon.

(U) The accusations came two days after an indictment in federal court in Alexandria, Va., accused fugitive Ayman Joumaa of leading a drug conspiracy that provided income for Hezbollah, an Iranian-backed Lebanese militant group that the United States has branded a terrorist organization. A Washington-based Drug Enforcement Administration spokesman told The Associated Press in February that Joumaa's organization laundered money using 50 used car lots in the United States. Cars were exported to Lebanon and West Africa.

(U) US Attorney Preet Bharara said the civil case reveals a massive international scheme in which Lebanese financial institutions, including banks and two exchange houses linked to Hezbollah, passed money through the US financial system to launder narcotics trafficking and other criminal proceeds through West Africa and back into Lebanon. The government said substantial portions of the cash were paid to Hezbollah, which has been designated by the US State Department as a terrorist organization since 1997. "The intricate scheme laid out in today's complaint reveals the deviously creative ways that terrorist organizations are funding themselves and moving their money, and it puts into stark relief the nexus between narcotics trafficking and terrorism," Bharara said. "Today, we are putting a stranglehold on a major source of that funding by disrupting a vast and far-flung network that spanned three continents."

(U) Hezbollah Demonstrates How Counterintelligence Analysis Can Get it Done (The *Denver Examiner, 01 DEC 2011*)

(U) As Sheik Hassan Nasrallah has so adamantly claimed in 2011, Hezbollah has partially uncovered the CIA's spy network in Lebanon. This has lead to the capture of several foreign spies working for the CIA in recent months and has damaged the intelligence agency's ability to gather vital information on the terrorist organization during a very tense time in the region.

(U) What makes it interesting is that Hezbollah beat the CIA at its own game, using methodical counterintelligence (CI) analysis and CI investigations to uncover the informants. The unit, which Nasrallah claims is a "spy combat unit," demonstrated how CI analysis and CI operations are supposed to function in order to protect an agency's information and how the CIA has not maintained a "greater awareness of counterintelligence," as former CIA director Leon Panetta said last year. As reported by the Associated Press in late November, CIA officials were warned their spies in Lebanon were vulnerable, and an ensuing study found weaknesses in intelligence operations there. Subsequently, recommendations were issued in order to create measures to counter the problems raised from Hezbollah counterintelligence efforts.

(U) Apparently this did not prove to be enough, though it is unclear if the new measures were in fact not successful or if Hezbollah simply followed older evidence created before the new measures were put in place by the CIA. Nevertheless, Hezbollah's unit tasked with CI proved that methodical analysis coupled with the financial support they receive from Iran can be a recipe to successfully combat the most powerful intelligence agency in the world. Reportedly, using only the latest commercial software, Hezbollah's CI analysts began methodically searching for traitors by first examining cell phone data and looking for anomalies. Then analysts identified cell phones that, for instance, were used rarely or always from specific locations and only for a short period of time. Then they underwent the tedious task of looking at who in that area had information that might be worth selling to the CIA, while others tracked CIA case officers who fell into predictable patterns when meeting their sources.

(U) Apparently the investigations took years, but eventually Hezbollah, and later the Lebanese government began making arrests, and regardless of whatever actions the CIA took, they were not enough. Bad tradecraft lead to the capture of CIA assets and ultimately the agency failed to protect them due to their inability to recognize Hezbollah counterintelligence operations.

PRESENTATIONS AND OUTREACH

The CI Strategic Partnership Newsletter is a product of the FBI's Counterintelligence Program Coordination Section which plays a key role in protecting our sensitive technologies from our adversaries.

The Challenge: to protect United States sensitive information, technologies and thereby competitiveness in an age of globalization.

Our Solution: to foster communication and build awareness through partnerships with key public and private entities, by educating, and enabling our partners to identify what is at counterintelligence risk and how to protect it. We call it "knowing your domain"—identifying the research, information and technologies that are targeted by our adversaries, and establishing an ongoing dialog and information exchange with partners, the goal of which is to change behaviors and reduce opportunities that benefit the opposition's efforts.

The United States is a world's leader in innovation. Consider the breakthrough research and development that's taking place on the nation's campuses and in research facilities—often on behalf of the government. Sensitive research, much of which occurs in the unclassified realm, is the key to our nation's global advantage, both economically and militarily.

The Counterintelligence (CI) Program Coordination Section is responsible for determining and safeguarding those technologies which, if compromised, would result in catastrophic losses to national security. Through our partnerships with businesses, academia, and US Government agencies, the FBI and its counterintelligence community partners are able to identify and effectively protect projects of great importance to the

U.S. Government. This provides the first line of defense inside facilities where research and development occurs and where intelligence services are focused.

The FBI's outreach efforts continue to evolve. This newsletter is one way we hope to expand our outreach to the elements of our "CI Domain." We continue in contacting businesses and organizations with which we have not yet made personal contact. In support of its Counterintelligence Domain/Strategic Partnership Program, the Federal Bureau of Investigation hosts an annual Research and Technology Protection (RTP) Conference for Facility Security Officers and RTP Professionals. Unclassified presentations address specific country threats to your technology, industrial and economic espionage, counterintelligence threat issues, and computer intrusion/cyber threat matters. The annual RTP Conference is offered in two locations during the year: Orlando and Clearwater.

The FBI's Domain/Strategic Partnership Program seeks to interface with private industry, high tech companies, research institutes, any stakeholder and/or contractor that design, develop, produce, and distribute critical information and technologies. Our job is to establish contact with these "Domain entities" in our territory, and assist them to better understand the foreign intelligence threat, and improve their ability to institute protective mechanisms. In addition to hosting an annual Research Technology Protection (RTP) Conference for security professionals, we also provide security awareness threat briefings to our defense contractor partners, high tech companies and research institutes. To schedule CI, cyber, security, education, training and awareness briefings, contact the Tampa Domain/SPC. You may also be interested in scheduling a presentation of the FBI video "BETRAYED" followed by Q&A.

"Betrayed" represents a scenario where an FBI Intelligence Analyst is slowly but steadly compromised by a series of steps that ultimately fully compromise him into working on behalf of a foreign intelligence service. The video clearly demonstrates the traits and activities demonstrated by individuals who are involved in stealing classified information (or even proprietary information and trade secrets). The video also shows the passivity of co-workers who have clearly seen demonstrations of suspicious activity by the Intelligence Analyst, and how their failure to report the suspicious activity exasperates the situation.

The Tampa Field Office Counterintelligence Strategic Partnership Program Coordinator:

James "Pat" Laflin (James.Laflin@ic.fbi.gov) 813.253.1029

Federal Bureau of Investigation

5525 West Gray Street
Tampa, FL 33609
Phone: 813.253.1000