Welcome to the Cyveillance Weekly Trends Report

Greetings from Cyveillance, the leader in open source threat intelligence. Since threat intelligence is constantly evolving, we publish this newsletter to keep our customers updated on the latest threats to various industries. Each week, we'll send you highlights from our analyst research reports. You can unsubscribe at any time. For the latest security news stories throughout the day, you can also follow us on Twitter, or to view the latest security articles from Cyveillance experts, subscribe to our blog.

In this Issue:

- Top Weekly Incidents
- Energy
- Agribusiness
- Insurance / Healthcare
- Financial Services
- Global Intelligence
- Legal and Regulations

New Whitepaper: The 2014 World Cup in Brazil: Examining Physical and Cyber Threats

From June 12 to July 13, Brazil will host the 2014 World Cup soccer competition. Learn more about the potential physical and cyber threats from terrorist and insurgent groups, disruptions from national and international activists, the impact of social media, and other security issues that may impact this event.

Click Here To Learn More

Top Incidents
Energy

- The 2014 Earth First! Round River Rendezvous will be held July 1st-7th. The annual summer Rondy will be in the Klamath-Siskiyou region of Southern Cascadia, roughly surrounding the border of so-called Oregon and California. Each Summer, this week-long camp-out attracts several hundred Earth First!ers from around the world. The gathering is coordinated by a volunteer committee and includes workshops, skill-shares, campaign discussions, story telling, campfire music and a rally with performers and speakers. This is a by-donation, rowdy, all-inclusive, backwoods event.

Agribusiness

- Business groups are urging longshoremen and their employers to avoid a dispute that could cripple ports along the West Coast and affect billions of dollars in commerce. A six-year pact between the Pacific Maritime Association and the International Longshore and Warehouse Union, which represents about 20,000 dock workers at 29 West Coast ports, expires June 30, both sides said in joint June 4 release. Negotiations began in May. The ports account for about half of all U.S. maritime trade and more than 70 percent of imports from Asia, according to the association.

Insurance/Healthcare

- Despite recent high-profile breaches, organizations are not buying cyber-insurance policies at explosive rates. The modest growth of organizations buying policies shows that they recognize that cyber-insurance is not the primary solution to how they should mitigate IT security risk.

Financial Services

- Mobile device management systems at a leading U.K. insurance company were last month hit by an attack based on the Heartbleed exploit that allowed hackers to compromise workers’ smartphones. The company was using BYOD service MobileIron to manage more than 1,000 smart devices. On the evening of May 20th, a hacker compromised the MobileIron admin server and posted a message to company-issued handhelds and respective email accounts. The hacker then performed a full wipe of every device and subsequently took out the MobileIron server itself.

Global Intelligence

- USA Today reported that a French company has launched an automatic application for the Right to be Forgotten in the European Union called forget.me. The site allows EU residents to apply to Google to have material removed from its EU search results. On 5/13/2014, Europe’s high court ruled that under European privacy laws, individuals have the right to request search engines to remove links to information that is “inadequate, irrelevant or no longer relevant,, or excessive in relation to the purposes for which they were processed.”

Legal and Regulations

- On June 19, 2014, the President’s Export Council (“PEC”) held a meeting to discuss nine key issues, including the effects of foreign laws that restrict cross-border data flows. At the meeting, the private sector members of the PEC submitted a recommendation letter to President Obama expressing their concern about the threat to American business from protectionist, cross-border data transfer restrictions imposed by foreign countries. The PEC, created in 2010, is the President’s principal national advisory committee on international trade. The PEC’s advice to the President focuses on domestic and foreign government policies and programs that affect U.S. trade performance and exports. In addition, the PEC provides a forum for business and government leaders to discuss and resolve trade-related issues.
The Pennsylvania Department of Health is being accused by two former employees who claim that the department placed gag orders on its employees, preventing them from talking about fracking to concerned residents.

A victory for the oil and gas industry in a pro-fracking vote in Loveland didn’t stop talk of a special legislative session to tackle new curbs on the practice in Colorado.

This article from RepublicReport.org discusses a growing trend throughout the country. Major players in the gas industry, which faces major regulatory hurdles relating to its extraction and distribution infrastructure, exports, and environmental issues, have taken to hiring the relatives of powerful politicians. In some cases, politicians with family ties to the gas industry hold sway over decisions critical to the industry.

Forbes.com reports that the Southwest Pennsylvania Environmental Health Project (SWPA-EHP) has been conducting a “pretty aggressive” indoor air monitoring project since 2011 in the midst of Pennsylvania’s gas drilling boom, particularly near unconventional wells that employed hydraulic fracturing, project director Reina Ripple said in a webinar hosted by the Natural Resources Defense Council. The project has documented sudden increases in particulate matter within homes, she said. SWPA-EHP employs a nurse practitioner who conducts exams and offers consultations at people’s homes and offices. In 2012-13, they determined 27 health complaints were likely attributable to gas drilling activities, including dermal, respiratory and neurological symptoms and eye irritation.

News article reports that the Supreme Court of Canada has granted declaration of aboriginal title to more than 1,700 square kilometres of land in British Columbia to the Tsilhqot’in First Nation, the first time the court has made such a ruling regarding aboriginal land.

TheEcologist.org suggests that since the natural gas industry is supported by the media, and politicians from across the spectrum, they are not beholden to average citizens.

The Colorado Oil and Gas Conservation Commission (COOGC) has directed High Sierra Water Services to stop disposing wastewater into a Weld County injection well as a result of a 2.6 magnitude earthquake striking the area Monday morning, about five miles away from Greeley, CO, the Colorado Independent reported. The earthquake marked the second one in just one month.

The British Medical Association (BMA) voted to end its investments in fossil fuels, becoming the first health-focused institution in the world to do so. Campaigners hope the vote will put the BMA in a strong position to advocate for other organizations to do likewise and end their support for companies driving “the greatest global health threat of the 21st century”.

Last week it was revealed that Greater Manchester Police spied on protesters at Britain’s biggest anti-fracking demonstration last year, using bugging devices and infiltrating them with undercover covert human intelligence sources. The action was revealed when the GMP didn’t realize that the official report released contained a glitch in their redacted text, which allowed anyone to view it simply by changing the color. It was further revealed that the drilling company being protested was being fed the covert information by the GMP.

The 2014 Earth First! Round River Rendezvous will be held July 1st-7th. The annual summer Rondy will be in the Klamath-Siskiyou region of Southern Cascadia, roughly surrounding the border of so-called Oregon and California. Each Summer, this
week-long camp-out attracts several hundred Earth Firsters from around the world. The gathering is coordinated by a volunteer committee and includes workshops, skill-shares, campaign discussions, story telling, campfire music and a rally with performers and speakers. This is a by-donation, rowdy, all-inclusive, backwoods event.

### Agribusiness

- Proponents of mandatory labeling for genetically engineered foods have spent $630,000 to collect signatures and get a ballot initiative before Oregon voters in November.

- The ongoing Western drought has landed every Utah county on a disaster declaration list from the U.S. Department of Agriculture.

- Business groups are urging longshoremen and their employers to avoid a dispute that could cripple ports along the West Coast and affect billions of dollars in commerce. A six-year pact between the Pacific Maritime Association and the International Longshore and Warehouse Union, which represents about 20,000 dock workers at 29 West Coast ports, expires June 30, both sides said in joint June 4 release. Negotiations began in May. The ports account for about half of all U.S. maritime trade and more than 70 percent of imports from Asia, according to the association.

- Activists destroyed experimental plots of rapeseed plants in southern France this week, the second razing in a month targeting field trials of mutated crops, national oilseed researcher Cetiom said.

- The EU has overtaken the USA to become the world’s top agricultural exporter.

### Insurance

- A new report indicates many vendors are missing even basic security technologies, and healthcare providers often aren’t forcing their vendors to meet the required standards.

- Device connectivity to a healthcare network continues to be a major issue in healthcare, and recent Wired report provides further insight into these vulnerabilities that, in some instances, can be remediated relatively quickly.

- A recent update to HHS’s public breach tool revealed an incident involving Salina Health Education Foundation (d/b/a Salina Family Healthcare Center) in Kansas. The April 8th incident affected 9,640 patients and was coded as “Unauthorized Access/Disclosure E-mail.”

- NRAD Medical Associates of Garden City, New York, has informed 97,000 patients that an internal employee inappropriately accessed protected health information (PHI) and patient billing data back in April 2014.

- The U.S. Attorney’s Office and justice department informed the Alabama State Department of Public Health they were prosecuting a case involving the theft of personal information. The Alabama Department of Public Health has indicated a breach of this magnitude is unprecedented at ADPH and that more than 500 people who visited one of the state’s 65 county health departments have been affected.

- According to the results of a recent survey of 100 senior IT security managers in the UK, 63 percent of respondents think it’s “easy” to govern staff access rights and privileges, even though 42 percent admit they don’t have, or are unsure of, the ability to monitor
and prevent breaches caused by accidental or deliberate staff actions

- Over 100 law enforcement officers fanned out Wednesday across Riverside County and made over a dozen arrests in an alleged auto insurance fraud ring involving fraudulent collision claims that bilked seven insurance companies out of more than $314,000.

- WellSpan Health has notified its employees about a situation that could expose the health system to a risk of federal health information privacy violations. Staff members were recently advised they could have unknowingly downloaded private patient information to their non-work devices.

- Despite recent high-profile breaches, organizations are not buying cyber-insurance policies at explosive rates. The modest growth of organizations buying policies shows that they recognize that cyber-insurance is not the primary solution to how they should mitigate IT security risk.

- The Montana Department of Public Health and Human Services (DPHHS) has reported more details on one of the largest HIPAA breaches in terms of the number of affected patients, as up to 1.3 million records were compromised. The server hack was first reported in early June when DPHHS hired an investigator and determined on May 22, 2014 that the server was likely accessed as far back in July 2013.

- Riverside County Regional Medical Center (RCRMC) has notified 563 patients that some of their personal data may have been compromised after a laptop computer was reported missing from a hospital procedure room late last week.

- Though medical device maker Medtronic revealed that hackers had entered its network on two separate occasions last year in its Securities and Exchange Commission (SEC) filing and didn’t steal anything, the incident appears to be in a bit of a compliance grey area. According to the Star Tribune, hackers from Asia were not able to steal any patient data, but Medtronic acknowledged that it has been unable to locate some patient records after hackers were able to access its diabetes unit network.

- An $800,000 HIPAA settlement between the Department of Health and Human Services and an Indiana community health system for an incident involving paper records dumping is the latest reminder that patient information needs to be safeguarded regardless of whether it’s electronic or paper-based.

- Colorado Neurodiagnostics of Littleton, Colo. is alerting an unknown number of patients that their protected health information (PHI) had been compromised when a laptop with the data was stolen from its office.

Financial

Activism

- Housing activists held a protest in Detroit, MI on June 24th outside a real estate development company to call for affordable housing in the area.

- A housing activist held a one-person, anti-foreclosure protest outside a leading U.S. bank branch on June 23rd in Fresno, CA.

- Occupy Wall Street is planning a five-day action event from September 17th through 21st in New York City with the intent to “…give the people the tools to engage in their own struggles against economic, social and political forces and injustices.”

- A ‘Student Debt Speak-Out’ took place in Philadelphia, PA’s LOVE Park on June 25th to
bring attention to eliminating student loan debt.

- Housing activists held an anti-eviction vigil against a government-sponsored enterprise for housing in Springfield, MA on June 24th to demand affordable housing and the end of forced evictions.

- Activists launched a petition against a leading U.S. bank to demand that the bank stop the “unlawful” eviction of a local resident in St. Louis, MO and rescind the foreclosure.

- Activists will hold an anti-bank rally on July 11th at the annual meeting of Uniform Law Commission in Seattle, WA, denouncing “a shady group of bank lawyers, attempting to enforce national uniform legislation to our state legislature.”

- Environmental activists held a protest against a leading Scottish bank outside its annual shareholders’ meeting that took place in Edinburg, Scotland on June 25th, demanding that the bank divest from the coal industry.

- Activists held anti-biofuel protests in London, UK on June 25th and Edinburgh, Scotland on June 26th, demanding that UK banks and government stop funding biofuel initiatives.

- Housing activists held an anti-eviction protest on June 25th in support of a local evictee in Atlanta, GA.

- Activists held a ‘Keeping Banks Accountable to Our Communities’ event on June 26th in Buffalo, NY to garner support for the campaign to pass a Responsible Banking ordinance in the City of Buffalo. A leading U.S. bank was accused of having over two thirds of the city's holdings, the highest minority lending denial rate, and not giving out business loans in the area.

- Activists held a protest on June 27th in the Detroit, MI Financial District against banks and corporations’ role in the "ongoing dismantling and destruction of the city."

- Housing activists will hold a rally at Los Angeles, CA City Hall on July 1st, demanding Los Angeles’ Mayor and City Council launch a public inquiry into all Wall Street dealings with the City of LA.

- Occupy Wall Street activists will participate in the 4th of July Main Street Parade that will take place in Santa Monica, CA to distribute flyers containing "important Occupy information."

**Information Security RisK**

- Researchers said a modification of the infamous CryptoLocker ransomware Trojan that neither relies on the 2048-bit RSA encryption nor communicates with a command and control server has been found in the wild. Although the GameOver Zeus botnet, also used by cybercriminals to distribute CryptoLocker ransomware, has been dealt a heavy blow by law enforcement agencies recently, variants of the file-encrypting malware are still available in the wild.

- Mobile device management systems at a leading U.K. insurance company were last month hit by an attack based on the Heartbleed exploit that allowed hackers to compromise workers' smartphones. The company was using BYOD service MobileIron to manage more than 1,000 smart devices. On the evening of May 20th, a hacker compromised the MobileIron admin server and posted a message to company-issued handhelds and respective email accounts. The hacker then performed a full wipe of every device and subsequently took out the MobileIron server itself.

- Hackers leveraged third party servers to launch DDoS attacks against a leading U.S. bank for four days.

- Hackers launched targeted DDoS attacks against Sri Lankan financial institutions under
the flag of #OpSriLanka due to the Sri Lankan Government's genocide of the Tamil minority.

- According to a report by a UK-based security firm, over the past two years, computer networks at dozens of banks, hedge funds, law firms, and other Wall Street companies have been infiltrated by hackers mainly from Eastern European countries.

- A leading provider of online real estate services was hit by a DDoS attack which has interrupted its websites' operations since it began June 17th. In connection with the attack, the website received a ransom demand.

- A Russian media source reported that sites of payment systems have become a common target of attacks by Russian hackers. The report adds that trading platforms and real estate sites are also a common target.

- Researchers said that by analyzing patterns in encrypted web traffic, attackers could gain insight to personal details of victims with 89% accuracy. The attack model consists of crawling the website to gather URLs and then analyzing them to produce a canonicalization function which, given a URL, returns a canonical label for the webpage loaded as a result of entering the URL into a browser address bar. The canonicalization function is then used to create a graph of the website. The researchers say their evaluation techniques bring an improved accuracy, to 89%, from the 60% recorded with other methods. Multiple leading U.S. based financial institutions’ websites were analyzed as part of the research.

- A vulnerability exists in the way a leading U.S. online payments and money transfer company handles certain requests from mobile clients and can allow an attacker to bypass the two-factor authentication mechanism for the service. This could also enable money transfers from a victim’s account to any recipient the threat actor chooses. The flaw lies in the way that the company authentication flow works with the service’s mobile apps for iOS and Android.

- Researchers identified a new Point-of-Sale malware dubbed ‘JackPOS.’ The new malware has unique attributes of custom pattern matching and its command-and-control (C&C) communication.

- A Citadel campaign that evaded the Microsoft takedown in June 2013 is now using the GameOver Trojan and is still claiming victims. The transition seems to have occurred before the disruption of the GameOver Zeus Trojan, dubbed Operation Tovar. Apart from info-stealing capabilities, the GameOver Zeus botnet also includes ransomware components (CryptoLocker) as well.

- Researchers identified a cloned banking app in a popular mobile application store that steals users’ credentials, but not their passwords. The malware, called ‘BankMirage,’ targets the customers of an Israeli bank. The authors put a wrapper around the bank’s legitimate app and redistributed it on the app store, pretending to be the financial institution. Once a victim opens the app, the malware loads the login form, which is an in-app html page that has been changed to siphon off the victim’s user ID’s as they enter their credentials. It’s effectively a phishing attack.

- A new study reveals that financial institutions, ePayment & Money Transfer Services, Social Networking sites, and Email services were the brand categories most frequently targeted by phishing kits, representing a combined 77% of kits analyzed. A phishing kit is a collection of files typically including web pages, images, scripts, and webserver code that can be installed on a webserver and ready to collect stolen credentials and other sensitive information quickly and with minimal configuration. Phishing kits are sometimes made available for free, but those often include backdoors that allow the kit’s author or distributor to receive copies of all stolen data or even take control over the server hosting the kit.
A new banking Trojan campaign dubbed ‘Luuuk’ stole €500,000 from 190 victims in Italy and Turkey in just one week.

Researchers said they have new evidence that more botnets and malware are being not only hosted in the cloud, but controlled remotely from cloud servers. The goal of hackers is to disguise their malicious software as regular traffic between corporate end points and cloud-based services.

**Legal, Litigation, Regulatory Risk**

- The Securities and Exchange Commission (SEC) will adopt a procedural rule regarding the submission of "substituted compliance" requests. This rule represents a first step in the SEC’s efforts to establish a framework to address the possibility that market participants may be subject to more than one set of comparable regulations across different jurisdictions as a result of their cross-border swaps activity. If the SEC were to grant a request for substituted compliance, it would permit market participants to satisfy certain Title VII security-based swap regulatory requirements by complying with comparable non-U.S. rules.

---

**Global Intelligence**

**China**

- On 6/27/2014, a Chinese news outlet reports several major World Cup lottery websites experienced DDoS attacks from unknown source during World Cup season.

- On 6/26/2014, a Chinese technology news outlet reports 7 types of malwares currently spreading among Android devices. The article also contains information regarding 10 malware category/families and 3 types of common methods of attack targeting Android devices.

- On 6/26/2014, a Chinese news outlet reports hackers targeting World Cup by releasing malicious mobile applications. Currently there are more than 375 malicious application related to World Cup.

- On 6/25/2015, a Chinese news outlet reports a trojan malware disguise as weather information application to lure users to download and install. Once infected, the malware will send out text messages to the user’s contact and causes an increase on user’s phone payment.

- On 6/24/2014, a Chinese news outlet reports an online game called “Phantasy Star OL2” experiencing massive DDoS attack from an unknown source since June 19th. The company has to delay the release of an update planned on June 25th.

- On 6/24/2014, a Chinese news outlet reports the research found that malwares related to mobile payment are targeting user under 18 due to low level of mobile security awareness.

- A Chinese news outlets reported that Foxconn’s Chongqing plant returned to normal operations following a worker strike last week. Foxconn parties stated that the company was able to reach an agreement on severance pay with workers. Due to decreases in laptop orders at the plant, Foxconn last week decided to lay off or transfer staff at their Chongqing plant.

- Over a thousand workers the Sambon Electronics plant in Dongguan went on strike demanding higher salaries. Workers expressed their discontent with overly long work hours, low wages, and high social welfare deductions from paychecks. Reportedly,
workers returned to work yesterday after the company agreed to raise salaries by 20 Yuan each month. Sambon Electronics is a Korea-based original equipment manufacturer (OEM) engaged in the manufacture of sound devices and keypads.

- The China Labour Bulletin reports that an arbitration committee in the central city of Changde has formally rejected a compensation claim by Walmart employees who were laid off by the company following a store closure in March. The local authorities meanwhile have been putting intense pressure on the workers to accept an unofficial settlement offer from Walmart of an additional 3,000 yuan each.

- Digitimes reported that Taiwan-based handset ODMs are losing orders from regional brands in Southeast Asia, Latin America, the Middle East and Europe to China-based rivals due to price competition and concerns of shipment volumes and inventory risks, according to sources. In addition to having strong production capacity, the China-based ODMs are also offering prices 10-30% below those offered by Taiwan-based ODMs, putting them at a major disadvantage to compete.

**Egypt**

- Journalists from all over the world are protesting the arrests of three Al Jazeera journalists in Cairo that took place this past Tuesday. BBC journalists and the Irish National Union of Journalists are amongst the most active protesters. The Al Jazeera journalists were sentenced to seven years for allegedly reporting false news and fabricating footage with regards to the 2013 coup that resulted in the ousting of president Mohamed Morsi.

**Germany**

- The implementation of IPv6 in German companies remains slow, despite the fact that the protocol is available for 15 years now and IP addresses are already a scarce resource. The problem will be even more pronounced with the advent of the “Internet of things”. One reason for the slow implementation seems to be the availability of workarounds like network address translating. Now a survey was launched to examine the general attitude of German companies towards the new technology, the progress in implementation, and to project future developments.

**France**

- USA Today reported that a French company has launched an automatic application for the Right to be Forgotten in the European Union called forget.me. The site allows EU residents to apply to Google to have material removed from its EU search results. On 5/13/2014, Europe's high court ruled that under European privacy laws, individuals have the right to request search engines to remove links to information that is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed."

**India**

- DNA India reported that cyber wing of Hyderabad Police has busted an illegal TV transmission racket. This racket was illegally tapping channels in India and abroad and being broadcast without permission. The individuals who were behind this activity caused an annual loss of rupees 6000 crore to the film industry and T.V. broadcasters.

**North America**

- According to Akamai, a leading cloud service, the global average web speed went up 24% annually to 3.9 Mbps, with 20% of connections now above 10 Mbps.

- USA Today reported that recently released numbers from some of the largest and most
powerful companies show that blacks and Hispanics are largely absent, and women are underrepresented in Silicon Valley, from giant companies to start-ups to venture capital firms.

- Forbes reported that more software programmers moved to Bangalore, India's technology hub, in the past year than the original Silicon Valley, says data by LinkedIn. While Bangalore clocked 44% new residents with technical talent, the San Francisco-Bay Area region had 31%.

- North Country Now reported that New York State Senator Joseph A. Griffo says the Senate has passed, with his help, a bill requiring employers to provide reasonable accommodations to employees with pregnancy-related medical conditions. Griffo says the bill imposes no hardship on employers, but "merely requires a reasonable accommodation - such as a foot stool to rest or an additional break for water."

- FEDweek reported that in a recent decision by the US Merit Systems Protection Board, an independent quasi-judicial agency established to protect federal merit systems against prohibited personnel practices and to ensure adequate protection for federal employees against abuses by agency management, recently overturned an initial decision that found disability discrimination and failure to accommodate a disabled employee resulting in her removal in Miller v. dept. of the Army. The case found that the employee refused viable reasonable accommodation options; as such, the agency was correct in subjecting her to a fitness-for-duty examination which found her disqualified for her position. According to the article, the case is a warning to employees who require accommodations to perform their jobs to be as flexible as possible in working out what accommodations will allow the workers to successfully perform their duties.

- The Times Union reported that Amazon, Microsoft and Boeing sweeten already lucrative job offers in Seattle with subsidized, furnished housing for interns. The article also cited free transportation anywhere in the country, including airport food, baggage fees and taxis as another perk for its intern.

- Times Union reported that there was a protest over Internet Neutrality at Google's headquarter in CA on 6/24/2014. The protest ended with the arrest of ten people on suspicion of trespassing.

- Inside Bay Area reported on several large acquisitions by Silicon Valley's tech companies. The article cited Oracle's recent acquisition of Micros System and Google's purchase of Dropcam, a San Francisco company that produces small cameras that can be accessed remotely from mobile devices for home security for $555 million.

- NBC News reported that a daughter of a Google employee wrote a letter to Google requesting that her father gets his birthday off from work. Google responded with a letter thanking the daughter for the note and gave her father the first week of July off as vacation time.

- "Bob Brown" on Bitmonger reported that user warned people that scammers may be taking advantage of an ISP's free WiFi hotspots to scam people out of personal information by setting up fake hotspots. According to the article, the scammers place wireless routers that broadcast wifi names to potentially gather users ISP passwords.

**Malaysia**

- On 6/24/2014, a Malaysian news outlet reports MTUC calling on the government to abolish the labor supplies system (contractor of labor) and review the recruitment on government-to-government basis to curb human trafficking.

- On 6/23/2014, a Malaysian human right activist named Charles Hector posted on his blog in response to the report regarding Malaysia being downgraded to Tier 3 in Human Trafficking Report of 2014 and blaming on Malaysia adopting contract-based-labor as
one of the main reason to this issue.

- On 6/22/2014, a Malaysian news outlet reports MTUC has proposed that minimum wage for private and public sectors to be raised to RM1,200 from RM900. MTUC claimed the current minimum wage of RM900 is too low and no longer practical due to rising cost of living.

**Vietnam**

- ChaoBuiSang.Net, a local VNese media source, reported that the U.S. based Microchip Technology Inc. is looking for a land to build a chip manufacturing plant in Ho Chi Minh City. The firm is seeking a location in the city that has complete infrastructure and trained workers for the project.

---

**Legal and Regulations**

- On June 19, 2014, the President’s Export Council (“PEC”) held a meeting to discuss nine key issues, including the effects of foreign laws that restrict cross-border data flows. At the meeting, the private sector members of the PEC submitted a recommendation letter to President Obama expressing their concern about the threat to American business from protectionist, cross-border data transfer restrictions imposed by foreign countries. The PEC, created in 2010, is the President’s principal national advisory committee on international trade. The PEC’s advice to the President focuses on domestic and foreign government policies and programs that affect U.S. trade performance and exports. In addition, the PEC provides a forum for business and government leaders to discuss and resolve trade-related issues.

**Financial Services**

- Industry experts are warning of an increase in cyber attacks on hedge funds in the wake of a major data breach recently reported by CNBC and verified by the cyber security firm BAE Systems Applied Intelligence. Hackers attacked a large hedge fund in late 2013, resulting in a significant security breach that passed information about trades to the hackers and disrupted the firm’s trading system, according to the recent CNBC report. BAE Systems, which investigated the breach for the hedge fund, has declined to comment on its client’s identity. The company did, however, tell CNBC that the attack cost the fund millions of dollars and suggested that it shows hackers are using increasingly sophisticated measures to wage cyber warfare against financial institutions. The breach occurred after hedge fund employees opened an e-mail that installed malware on their computers. The program delayed the execution of trades by milliseconds and sent some trade details to outside sources. The amount of profits earned by the hackers in this breach is unknown. Hedge funds and other financial institutions should be prepared for hacking attempts. Companies can assess their own preparedness using an SEC form designed to evaluate cyber security risk or the NIST framework, and should proactively establish procedures to deal with the myriad reporting, notice, and other obligations that may arise in the wake of a data breach.

**Pharma**

- A federal court has upheld the validity of the FTC’s recent rules for reporting certain transfers of exclusive patent rights in the pharmaceutical industry under the Hart-Scott-Rodino Antitrust Improvements (“HSR”) Act. These rules require that an HSR filing be made for transfers of exclusive patent rights constituting “all commercially significant rights” in the pharmaceuticals sector that meet the other HSR criteria. A pharmaceuticals trade association challenged these regulations under the Administrative Procedures Act. On May 30, the court issued a seventy-page opinion rejecting this challenge and keeping the FTC’s rules intact and in full force.
Cyveillance, Inc.
11091 Sunset Hills Road Suite 210
Reston, Virginia 20190

www.cyveillance.com
Contact Us
+888-243-0097

Copyright © 2014 Cyveillance, Inc.