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

Social Media Watch: Cyveillance now offers services designed to help smaller organizations, particularly banks and credit unions, monitor social media for risk and compliance. Cyveillance Social Media Watch leverages the same proprietary platform, reporting capabilities, and in-depth analysis that power solutions for Fortune 500 customers, but is scoped to address the budgets, needs, and risks of smaller companies. Service elements include Monitoring, Vetted Alerting, Incident Investigation Reports, and Global Intelligence.

Top Incidents

**Energy**

- Environmental activist group Deep Green Resistance has published a new manual, titled Decisive Ecological Warfare. The group strongly implies that the new manual adapts to the environmental movement the asymmetric warfare techniques taught in conventional military colleges.

**Agribusiness**

- The Organic Consumers Association has urged consumers in every state to...
band together to defeat the impending lawsuit brought forth by the Grocery Manufacturers Association against GMO labeling in Vermont. Organic Consumers Association further calls readers to pressure institutional investors to dump stock in GMA companies and impose a boycott on GMA company products.

**Insurance/Healthcare**

- With the mandated adoption of electronic health records (EHRs), many healthcare professionals for the first time got centralized access to patient records. Now they're figuring out how to use all this information. Although the healthcare industry has been slow to delve into big data, that might be about to change. At stake: not only money saved from more efficient use of information, but also new research and treatments -- and that's just the beginning.

**Financial Services**

- A hacker group behind operation #TheWeekOfHorror published a list of banks to be targeted by DDoS attacks during their operation, which is set to launch in July 2014. The group notes that in addition to targeting the US's financial sector, it will also seek to control of air-traffic computers and key systems in the energy sector.

**Global Intelligence**

- A Chinese news outlet reports trojan malwares disguised as World Cup application spreading rapidly in China targeting mobile devices as well as computer in order to obtain users' information.

**Legal and Regulations**

- In a landmark case for the future of digital privacy, Europe’s highest court ruled on May 13, 2014 that internet search engines, such as Google, can be required to block access to search results about individuals at their request. The ruling of the Court of Justice of the European Union in Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González has the potential to drastically alter the privacy landscape. It will allow individuals to assert their right under EU data protection law to require search engines to rectify, erase or block access to search results about them where these are incomplete, inaccurate, irrelevant or outdated or otherwise breach EU data protection law, whether or not they cause prejudice to the individual.

**Energy**

- Resources company Metgasco’s plans to drill for gas at Bentley on the NSW north coast (Australia) are in disarray after state energy minister Anthony Roberts referred the project to the Independent Commission Against Corruption and announced its license would be suspended due to insufficient community consultation. The blockade was scheduled to be disrupted by over 800 police officers this week, so activists are considering this a major victory.

- Anger and grief have boiled over into violent protests in several parts of Turkey after a mine disaster killed at least 274 people. Turkish police on Wednesday fired tear gas and water cannon at thousands who were protesting in Ankara's downtown Kizilay square. Similar protests were taking place in Istanbul’s iconic Taksim Square and in the western town of Soma, where the explosion at a coal mine triggered a deadly collapse. Scores of workers remained trapped inside the mine.

- New evidence suggests that oil and mining protests from local people are effective,
extremely costly for the companies, and often lead to substantive changes to or total abandonment of a project. Researchers at the Centre for Social Responsibility in Mining interviewed employees at several dozen major international corporations who are involved with extractive activities, and found that companies are increasingly having to deal with the social and environmental impacts of their work, and that it’s hurting them where it hurts most: their bottom lines.

- The Los Angeles Fire Department says a ruptured oil pipe has caused about 10,000 gallons of crude oil to spill on to the city's streets. The oil - which covers a half-mile area and is knee-high in some places - escaped after a break in an above-ground pipeline outside 5175 West San Fernando Road in the Atwater Village suburb. According to Los Angeles Fire Department, oil was spurting 15 to 20 feet into the air from a burst 20-inch pipe, with the leak reported shortly after midnight local time.

- The EPA is taking steps toward having companies who "frack" disclose the chemicals used in that operation. The site notes that the EPA has not yet drafted a proposed regulation, but said in the notice that it will consider both mandatory and voluntary rules. Among other things, the EPA will consider requiring disclosure of the identity, amount, type, and circumstances of use for the chemical substances and combinations used in the hydraulic fracturing process. Also on the table are health and safety studies relating to particular chemicals or chemical combinations.

- The Augusta Chronicle reports that a federal nuclear safety oversight panel has warned the U.S. Department of Energy that an apparent spike in safety violations, contamination incidents and injuries at Savannah River Site must be addressed before a more serious incident occurs. In a safety report for the week ending April 4, the Defense Nuclear Facilities Safety Board found an uptick in safety concerns during the first quarter of 2014. Site contractors Savannah River Nuclear Solutions and Savannah River Remediation and DOE have been trying to make corrective actions, according to the report. Below the article several readers have commented. One reader comments that they worked at SRS back in the early 90's and that back then safety procedures were routinely ignored.

- The activist who coined the term "Thin Green Line" to describes the Pacific Northwest's efforts to stop energy exports travelled to Canada to speak against energy exports in British Columbia.

- Criminal negligence charges have been brought in the case of the oil train explosion that took place last year in Lac-Megantic in eastern Quebec. This explosion has become a galvanizing symbol driving oil train concerns and anti-oil train activism in both Canada and the United States.

- The 3rd edition of the Earth First! Direct Action Manual is being released, and publishers are organizing a book tour emphasizing arranging "trainings aimed at teaching some of the direct action skills discussed in the DAM."

- The 2014 Heartwood Forest Council, “A Climate of Extraction,” will be held Friday-Monday, May 23-26 at Camp Ondessonk, near Stonefort in the heart of the Shawnee National Forest in Southern Illinois.

- A new coal export terminal has been proposed in Mexico. The terminal would primarily ship Powder River Basin coal, and is likely inspired by the failure of 3 (so far) of the 6 proposed PNW coal export terminals. Organized grassroots oil train opposition in California's numerous refinery communities will likely become a larger, organized grassroots force that also opposes coal trains if this proposal gains momentum.

- The Chinese government has sent an offshore oil rig into territorial waters claimed by both China and Vietnam, dubbing the rig “mobile sovereign territory.” This has elevated tensions to such a degree that a thousands-strong Vietnamese mob rampaged, setting
Taiwanese factories ablaze in industrial zones in southern Vietnam.

- Environmental activist group Deep Green Resistance has published a new manual, titled Decisive Ecological Warfare. The group strongly implies that the new manual adapts to the environmental movement the asymmetric warfare techniques taught in conventional military colleges.

- U.S. Sen. Barbara Boxer (D-CA), Chairwoman of the Environment and Public Works Committee, Senator Bernie Sanders (I-VT) and Senator Edward J. Markey (D-MA) introduced three bills aimed at improving the safety and security of decommissioning reactors and the storage of spent nuclear fuel at nuclear plants across the nation. The three bills address safety of spent fuel storage and decommissioning plans. They are entitled: Safe and Secure Decommissioning Act of 2014; Nuclear Plant Decommissioning Act of 2014 and Dry Cask Storage Act of 2014.

- Rising Tide Seattle protested this week calling for a moratorium on oil trains at the screening of “Years of Living Dangerously” where WA Governor Jay Inslee was in attendance. The protesters used exploding train props and unfurled a banner from the balcony of the cinema.

### Agribusiness

- In Venezuela, lack of access to US dollars and government control of pricing, among other policies are worrying to many international food industry companies with sizeable operations in the country, including Nestle, Cargill, General Mills, and Mondelez International. In their first quarter filing with the SEC, Heinz flagged these issues in the country as well as it’s “highly inflationary” economy.

- The Organic Consumers Association has urged consumers in every state to band together to defeat the impending lawsuit brought forth by the Grocery Manufacturers Association against GMO labeling in Vermont. Organic Consumers Association further calls readers to pressure institutional investors to dump stock in GMA companies and impose a boycott on GMA company products.

### Insurance

- As the HITECH Act electronic health record incentive program enters its final phases, federal regulators are weighing changes to the EHR software certification requirements, as well as the “meaningful use” requirements for hospitals and physicians.

- The personal information of approximately 3,500 members of the New Zealand Dental Association (NZDA) appears to have been accessible online for more than a year.

- With so much PII data floating around, details can easily be cross-correlated, helping criminals quickly put together accurate identity profiles. With just a few pieces of “secret” personal information, thieves can potentially gain access to online accounts, and even financial accounts, through identity theft.

- The University of California – Irvine is notifying patients of a data security breach involving their medical information. In late March, UC Irvine discovered that several computers in the UC Irvine Student Health Center had been infected with a keystroke logger that captured data as it was entered onto them and transmitted that data to unauthorized servers. UC Irvine believes that the following types of patient information
were captured and exfiltrated: name, unencrypted medical information (potentially including health or dental insurance number, CPT code(s), ICD9 code(s) and/or diagnosis), student ID#, non-student patient ID#, mailing address, telephone #, amount paid to the Student Health Center for services received, and bank name and check # (if payment was made by check).

- Boulder Community Health (BCH) of Colorado is in the process of investigating its third patient data breach since 2008, according to The Daily Camera. The context of the breach is a bit bizarre in that, unknown to BCH, someone mailed patients’ records to their homes to prove that BCH is lacking in security.

- With the mandated adoption of electronic health records (EHRs), many healthcare professionals for the first time got centralized access to patient records. Now they’re figuring out how to use all this information. Although the healthcare industry has been slow to delve into big data, that might be about to change. At stake: not only money saved from more efficient use of information, but also new research and treatments -- and that’s just the beginning.

- Federal authorities announced May 13th that charges have been filed against 90 individuals in six states who are allegedly tied to Medicare fraud schemes responsible for $260 million worth of false billings.

- Among those charged as a result of the federal government's Medicare Fraud Strike Force investigation are 27 physicians, nurses, and other medical professionals in Michigan, Florida, California, New York, Louisiana and Texas.

- Eastern Health reported Tuesday that an employee inappropriately accessed 20 patient records in a privacy breach. According to a release from the health authority, the administrative employee has resigned in light of the investigation. Eastern Health said it has identified all of the patients affected, and will make contact to advise them of the deliberate breach.

- Comfort Insurance, a leading motorhome insurance provider, warns drivers about an accident insurance scam named ‘smash for cash.’ This tactic can net criminal gangs thousands of pounds, whilst risking injury or even death to innocent victims. Comfort Insurance has had a number of cases over the last year which were believed to be a case of smash for cash, although it has been almost impossible to prove. Therefore, the claims have been put forward as “at fault,” resulting in customer’s premiums increasing. Comfort Insurance looks at smash for cash and how motorists can protect themselves from the scam.

- A federal district judge has dismissed the majority of a consolidated class action lawsuit that was filed against TRICARE, the military health program, and Science Applications International Corp. in the wake of a 2011 data breach that affected nearly 5 million individuals. The incident is the largest data breach reported to federal regulators under the HIPAA breach notification rule.

- Employees affected by the University of Pittsburgh Medical Center (UPMC) data breach have filed a class action lawsuit against UPMC and its payroll vendor, Ultimate Software Group. The suit says that UPMC and the vendor breached its duty to protect private employee information and exposed those employees to tax return fraud.

- The Department of Health and Human Services (HHS) releasing its Security Risk Assessment Tool has spurred diverse opinions as to how healthcare organizations should use the tool as part of their compliance strategy as well as audit preparation.

- Nearly all states collect hospital discharge data, with 33 states selling or sharing de-identified information--not covered under HIPAA. That raises concerns that the
hospitals are turning over data potentially vulnerable to re-identification, according to the Federal Trade Commission.

- Los Robles Hospital And Medical Center in Thousand Oaks, California, notified 2,523 patients of a breach involving their business associates, Courier Express/Atlanta, Courier Express/Charlotte & Courier Express US, Inc. The breach, which occurred on February 14th, was reported to HHS as involving “Theft, Unauthorized Access/Disclosure” of paper records.

- For the second time in five months, patients’ information may have been compromised in a data breach at nine Washington hospitals that make up the Franciscan Health System, which is part of the national Catholic Health Initiatives (“CHI”). CHI has filed a lawsuit in order to submit a legal request to Microsoft to provide information about the email accounts used in the hacking; the lawsuit alleges that, during five days at the end of March, a hacker was able to redirect a significant number of emails sent to doctors and staff from patients and laboratories. Instead of getting to the intended recipients, those emails were directed to the hacker’s account. The lawsuit also states that the hacker gained control of domain names like catholichealth.net.

Financial

Activism

- Activists protested outside a leading U.S. bank branch in Rahway, New Jersey on May 13th, demanding the city government move their money into local banks.

- Housing activists held a protest outside the demolition site of a home in Seattle, Washington that was recently foreclosed on by a leading U.S. bank.

- Housing activists launched a Facebook event page to gain support for a petition and the eviction defense of a local resident in Lithonia, Georgia who is facing an alleged illegal foreclosure by a leading U.S. bank.

- A former employee of a leading U.S. bank held a protest outside the bank’s branch in New York City on May 12th and 13th, threatening to file a lawsuit against the company.

- Activists held a protest at a major UK bank’s shareholders’ meeting in Edinburgh, UK on Thursday May 15th, accusing the bank of “destroying people’s lives and fuelling climate change by bankrolling the global coal industry.”

- Activists have launched a petition against a leading U.S. investment firm, demanding that it divest from a mining exploration project in Guatemala due to “ongoing violence and broad local opposition.”

Information Security Risk

- A hacker group claimed to have downed the website of bank in Mexico on May 9th.

- A hacker group claimed to have downed the website of the Central Bank of Cambodia on May 8th.

- A domain hosting service provider suffered a major outage on May 9th after it was hit
with a serious DDoS attack on all of its DNS servers. The firm is responsible for more
than 220,000 domains worldwide. The attack is believed to have originated from China.

- A hacker group behind operation #TheWeekOfHorror published a list of banks to be
targeted by DDoS attacks during their operation, which is set to launch in July 2014. The
group notes that in addition to targeting the US’s financial sector, it will also seek to
target control of air-traffic computers and key systems in the energy sector.

- Researchers say hackers have been stealing Google account passwords in a new and
better crafted phishing attack that is hard to catch with traditional heuristic detection.

- Researchers claim there are at least 21,000 vulnerable servers in the Netherlands which
are holding personal information.

- Researchers say small companies are on the front line of a credit card hacking boom
and face serious costs if their lax systems allow customer data to be lost. Electrical
retailers have been hit with more breaches than any other sector, followed by general
retail and clothing.

- Newly released allegations by Edward Snowden claim the NSA routinely intercepted
US-made routers bound for export and planted backdoors on them.

- Researchers say over the last several years, PoS attack campaigns have evolved from
opportunist attacks involving crude theft of card data with no centralized command and
control. They morphed into memory-scraping PoS botnets with centralized C&Cs, and
most recently have become highly targeted attacks that require a substantial amount of
lateral movement and custom malware created to blend in with the target organization.

- The United States Postal Inspection Service is investigating reports that fraudsters are
installing skimming devices on automated stamp vending machines at Post Office
locations across the United States.

- Researchers warn that although the backdoor, Xtrat, is a relatively old piece of malware,
many AV (anti-virus) vendors are still not consistently detecting it because attackers
consistently alter the binary and there are numerous variants.

- The Commodity Futures Trading Commission said they plan to weed out any unfair
advantage speed traders may have by getting sensitive information ahead of others.
CFTC staff is considering whether to draw up rules for automated trading after receiving
comments from market participants on a so-called concept release, often a first step
towards new regulations.

- UK public sector bodies are being warned that they could face cyber-attacks within days
as a result of growing tensions in Ukraine. An Internet security firm has issued a threat
alert which says that NATO countries, particularly the UK, Germany and France, along
with the US should increase their readiness levels to cope with any such incidents.

- Adobe has released security updates to address a total of eleven vulnerabilities affecting
the Mac and Windows versions of Adobe Reader and Acrobat 11.0.06 (XI) and earlier.
The company has also fixed six security holes affecting Adobe Flash 13.0.0.206 and
earlier variants for Windows and Mac. The vulnerabilities are considered critical and
they’ve been assigned a priority rating of 1, which means that they’re either being
targeted, or they have a high risk of being targeted. Adobe recommends system
administrators to update installations as soon as possible, preferably within 72 hours.

- Microsoft has released updates to address vulnerabilities in Windows, Office, Internet
Explorer, Server Software, Office Services, Web Apps, and Productivity Software as part
of the Microsoft Security Bulletin Summary for May 2014. These vulnerabilities could
allow remote code executions. US-CERT encourages users and administrators to review the bulletin and apply the necessary updates.

- Researchers say cybercriminals are maturing their "weaponization" of email bornbs, with sophisticated malware and “blitzkrieg” attacks designed to steal personal information, extort money and destroy trust between businesses and customers.

- Researchers claim the National Security Agency is able to work around Skype's encryption system and access users' buddy lists, credit card information, call records, user account data, and "other material."

- Researchers say the gang behind Zeus, also known as Gameover, had used new Webinjests against 1,515 unique targets during the first three months of the year; up from nearly 1,100 in January 2014. Most of the new targets were banks and financial institutions in Africa, the Middle East, Asia and Europe. The gangs maintaining and selling Zeus are improving the Webinjests used by the malware to update infected computers on the fly.

- Experts say Silicon Valley tech companies are under attack by groups and foreign countries probing for potential vulnerabilities in new Internet technology. The nature of cyber-attacks are changing, involving highly trained operators from other nations and sophisticated groups of criminals who are winning the battle against the defenders of the information network.

- MyFox9 News reported that some major retail websites have a security glitch that could put customers' personal information in the wrong hands, allegedly, one of these sites includes Target.com. After the Target breach during the last Black Friday holiday shopping season, a local security expert now says a "misconfiguration of encryption software" could allow hackers to use stolen information to go on shopping sprees online and leave unsuspecting customers with the tab.

**Legal, Litigation, Regulatory Risk**

- A total of 13 individuals were arrested since the end of January 2014 by Dutch and Belgian authorities as part of an investigation targeting a cybercriminal organization. Belgium's federal prosecutor has been collaborating with Eurojust and Dutch law enforcement agencies to bring the alleged members of the crime ring to justice. The group relied on phishing and vishing (voice phishing) to trick their victims into handing over the information needed to access their bank accounts.

- Bank of England’s deputy governor for financial stability warned that the issue of banks being 'too big to fail' remained and additional requirements being introduced by the regulators were necessary.

- A former owner of several fast-food restaurants in southern California pleaded guilty Wednesday to charges stemming from a gift card scheme that involved tampering with several other stores' computerized cash registers. Federal prosecutors accused the former owner of selling point-of-sale systems to at least 13 fast-food stores with remote login software called LogMeIn installed.

**Operational Risk**

- A popular Bitcoin service firm confirmed last week that their systems were hacked by cybercriminals, and customers' deposits were stolen.

- Nearly 300 complaints were filed with the Federal Trade Commission (FTC) against a Bitcoin-miner maker in Kansas. The company has faced numerous accusations of fraud. Currently, the company is battling one lawsuit in federal court with more likely on the
A trading firm’s mistake caused wild price swings in U.S. stocks about 10 minutes before the markets closed on May 13th. The shares were moved by orders tied to the close of trading that were incorrectly entered.

Shares of an investment management and financial planning firm lost 7.4p to 320p after it announced the cancellation of the roll out of its back office IT system that will result in a one-off £32million non-cash write-off of capitalized IT costs.

Reputational Risk

An article published on the website of an American politically progressive/democratic socialist monthly magazine claims the city of Los Angeles pays $300 million a year on financial fees, $200 million of which goes towards paying the fees of Wall Street money managers that oversee some of the city’s pension investments. Further, the article notes LA is "now on the hook for $65.8 million worth of new fees in the next 14 years, thanks to a 2006 interest-rate swap deal."

An online article published by a major U.S. newspaper last week contained commentary regarding the negative reactions shown by attendees' at the shareholders’ meeting of a leading U.S. bank held two weeks ago in Charlotte, North Carolina. One attendee noted her displeasure with the bonus given to the bank’s CEO and the lack of handicapped parking at her local bank branch.

An article published last week claimed that 401ks are being used by politicians, Wall St., and the Koch brothers to drain Social Security. The piece posits that conservative lawmakers and supporters have been seeking to phase out Social Security and address retirement planning through private fund companies. The piece also asserts that were this to happen, it would in effect pass all retirement accounts into the hands of Wall St. executives, and also expose individuals retirement money to an inherently volatile stock market.

Global Intelligence

China

A Chinese news outlet reports trojan malwares disguised as World Cup application spreading rapidly in China targeting mobile devices as well as computer in order to obtain users' information.

Sina Tech news reported that Taiwanese-owned Jian Ding Electronics (Wuxi) caught fire on Fri, May 9th. According to a preliminary investigation, the fire was caused by an exhaust pipe. Jian Ding Electronics in Wuxi is one of the world’s top manufacturers of printed circuit boards (PCB).

Chinese news outlets reported a strike of hundreds of workers which broke out on May 14th at Nokia’s assembly plant in Dongguan. Workers went on strike when they feared they would not receive proper compensation following Microsoft’s purchase of the factory. Nokia plant officials stated that the labor disruption has not negatively impacted business operations.

Chinese news outlets reported that on Monday May 14th, workers at Dynacast factory in Shanghai started a strike against year-end bonus in arrears and abusive penalty policies. Police intervened and several workers were reportedly beaten as police attempted to gain control of the situation. In addition, 33 were arrested. Dynacast is a
global manufacturer of metal components and a leader in multi-slide zinc die casting technology, conventional zinc die casting and precision aluminum die casting.

Germany

- The German Federal Police (Bundeskriminalamt, BKA) cautions against a cyber-threat specifically targeting mobile online banking in Germany. One-time passcodes (so-called transaction numbers or TAN) are widely used in Germany for online banking to authenticate a customer’s transaction request. The mobile or mTAN process requires a customer to verify a transaction by using a passcode which is sent by the bank to the customer’s cell phone. Cyber criminals are using manipulated cell phone apps to intercept and read those passcodes. During the first quarter of 2014, the number of attacks using the malware Faketoken increased alone over six times.

North America

- From June 27-30, 2014 in Washington, DC, the Humane Society USA will be holding its largest conference, Taking Action For Animals. The conference will be attended and/or sponsored by a number of other activist groups and NGOs including Mercy For Animals, Big Cat Rescue, Farm Sanctuary, National Canine Research Council, World Society for the Protection of Animals, etc.

- On Thursday May 14, 2014, nationwide protests against the Federal Communications Commission (FCC) took place in regards to newly unveiled internet regulations. The protests come amidst the FCC’s decision to end net neutrality, thus making it possible for internet service providers (ISP) to charge companies like Netflix for faster internet speeds. Members of MoveOn.org, CREDO Action and Free Press gathered around offices in 24 regional FCC locations to protest the new regulations.

- ZDNet reported that after years of denying responsibility, Samsung now promises to offer adequate compensation for employees who died of or developed leukemia from working at the company’s semiconductor plants.

- CBS News reported that over one hundred protesters organized outside Google’s annual shareholder meeting at Google’s Mount View headquarters on 5/14/2014. The protesters ranged from housing rights advocates from San Francisco to consumer watchdogs concerned about Google’s tax policies. About five of the protesters had proxies who went in to speak at the meeting.

- Hot Brands reported that on plaintiff in the Silicon Valley hiring scandal is asking the judge to reject the settlement reached by the four firms accused in the case. The plaintiff believes that the tech companies are getting off too easily and he sent a letter to the judge handling the case asking her to reject the deal.

Vietnam

- Yahoo News reported mobs torched and looted scores of foreign-owned factories in Vietnam following a large protest by workers against China’s recent placement of an oil rig in disputed Southeast Asian waters. The unrest occurred at industrial parks close to Ho Chi Minh City.

- Reuters reported that up to 21 people were killed in Vietnam and a huge foreign steel project was set ablaze as anti-China riots spread to the center of the country a day after arson and looting in the south. Thousands of Vietnamese set fire to foreign factories and rampaged through industrial zones in Binh Duong and Dong Nai provinces near Ho Chi Minh City on Tuesday, officials said. Protests continued on Wednesday. Hundreds of Chinese working in the zones have fled, most to neighboring Cambodia and others by air.
Vietnam+ reported that Chairman of Ho Chi Minh City’s municipal People’s Committee held a May 15 working session with representatives of some foreign consulate generals based in the city regarding recent incidents in Ho Chi Minh City and surrounding localities during which some extremities had destroyed the property of foreign enterprises. Municipal leaders have instructed authorized agencies to ensure the safety of foreign businesses. The city has directed IZ and EPZ management boards to immediately repair damaged fences and facilities.

Nguyen Tan Dung, a local VNese media source, reported that for the first time the Revised Labor Code has included a proposal for paternity leave in VN. If the National Assembly accepts the proposal, male workers will be able to take 5 to 7 days paid paternity leave.

Nguoi Lao Dong News, a local VN media source, reported 50 workers from Van Company, a cargo loading and unloading company, went on strike. Employees complained that they had to work overtime often without proper compensation. In addition, the company’s failure to sign labor contracts and pay for health and social insurances caused employees to be unable to receive workers’ benefits.

ChaoBuoiSang.Net, a local VNese media source, reported that IBM on 5/12/2014 launched a counseling program on technology application and management for Dong Nia’s Department of Health and Department of Science and Technology.

---

**Legal and Regulations**

**Financial Services**

- On May 6, New York Governor Andrew Cuomo announced the release of “The Report on Cyber Security in the Banking Sector” which surveyed 154 depository institutions in New York, including regional banks, credit unions, and branches and agencies of foreign financial institutions regarding their cybersecurity programs, costs, and future plans. Most significantly, Cuomo also announced that the state’s Department of Financial Services will begin auditing the cybersecurity systems of regulated financial institutions.

**Global Intelligence**

- In a landmark case for the future of digital privacy, Europe’s highest court ruled on May 13, 2014 that internet search engines, such as Google, can be required to block access to search results about individuals at their request. The ruling of the Court of Justice of the European Union in Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González has the potential to drastically alter the privacy landscape. It will allow individuals to assert their right under EU data protection law to require search engines to rectify, erase or block access to search results about them where these are incomplete, inaccurate, irrelevant or outdated or otherwise breach EU data protection law, whether or not they cause prejudice to the individual.

- Brazilian Congress passed the “Internet Bill of Rights.” The legislation, which passed the Brazilian Senate unanimously in April, is intended to secure equality of access to the Internet in Brazil—the Net Neutrality—and provide privacy protections for Brazilian users of the Internet. Companies that collect personal data from residents of Brazil will be subject to Brazil’s laws and courts in cases involving information on Brazilians, even if the data is stored on servers abroad.