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 /Pharmaceutical
- Financial Services
- Global Intelligence
- Legal and Regulations

New Webcast:

Webcast: Concrete Steps to Deploy an Effective Threat Intelligence Capability
Part II of a Two-Part Series on Threat Intelligence

Eli Chen
Director of Product Strategy
dcchen@cyveillance.com

July 16th
1:00 PM

Protecting your business —

including its information and

intellectual property, physical infrastructure, employees, and reputation — has become increasingly difficult. Among thought leaders and advanced organizations, the consensus is now clear. To adequately protect company assets and ensure business continuity, organizations must be more proactive and make effective use of threat intelligence.

Click Here To Learn More

Top Incidents
Exxon Mobil Corp. is fighting criminal charges over a wastewater spill in Pennsylvania with an unusual defense, contending that the state's attorney general has improperly singled it out in a bid to stop fracking. On Wednesday, Attorney General Kathleen Kane fired back with a legal response, calling the company's claims "nothing more than weak attempts to obfuscate the truth." Prosecutors say an Exxon subsidiary, XTO Energy Inc., is criminally liable for a big leak of water that had been used in hydraulic fracturing, or fracking, in north-central Pennsylvania in 2010.

A large umbrella group of churches representing more than half a billion Christians worldwide announced Thursday that it would pull all of its investments in fossil fuels, saying it had determined the investments were no longer ethical. The World Council of Churches, a global coalition of 345 churches, made the decision to no longer fund oil, gas, or coal at its central committee meeting in Geneva, and recommended that its members do the same.

A study released last week reported that the last five years have seen Oklahoma experience more than 2,500 earthquakes – the vast majority of which are being connected to the oil and gas exploration process of fracking. Although past studies have also suggested Oklahoma's earthquake spike is related to fracking, this is the first time scientists have pinned such numbers to the controversial procedure.

This is a petition aimed at large media corporation requesting them to air a PSA critical of Exxon. The page explains that this group had paid for a similar PSA previously, and that afterwards the media company received letters from Exxon. The activist group believes that since no media outlet will air their PSA that Exxon must have something to do with it.

The Vancouver Sun reports that the hereditary chiefs of the Gitxsan First Nations served notice Thursday to CN Rail, logging companies and sport fishermen to leave their territory along the Skeena River in a dispute with the federal and provincial governments over treaty talks. And the Gitxaala First Nation, with territory on islands off the North Coast, announced plan to file a lawsuit in the Federal Court of Appeal on Friday challenging Ottawa's recent approval of the Northern Gateway pipeline from Alberta.

The Texas Tribune reports that after watching a $5 million grant to Gov. Rick Perry's office go unspent nearly four years after it was presented in the wake of the April 2010 Deepwater Horizon explosion and oil spill in the Gulf of Mexico, BP is asking Texas for its money back. The funds were given to Texas in September 2010 to help with oil spill recovery, but few of the state and local officials who work on such projects were aware of the grant until a legislative hearing in May. Lawmakers at the hearing were angered and said the money should have been given to agencies with the expertise to spend it. BP was frustrated as early as last winter about the unspent funds and asked Perry to return the money, according to correspondence obtained by The Texas Tribune through an open records request.

Operating cost data from participants in a power network stretching from the Midwest to the Gulf Coast was compromised in a computer breach that highlighted the rising vulnerability of the U.S. electricity infrastructure. Midcontinent Independent System Operator Inc. said it was notified June 26 that a computer server tied to its independent monitor was breached. MISO, based in Carmel, Indiana, said it reported the intrusion to FERC and began investigating. While the perpetrator could have seen the market data on the affected server, there is no indication that happened.

Progress Florida has created a petition addressed to the Florida Legislature urging them to ban fracking in Florida. "We the undersigned urge you to put a stop to the unsafe oil
and gas extraction process known as fracking, including a new form of drilling happening in the Everglades known as acid fracking. The last thing Florida needs, with our delicate ecology and vast underground aquifer system, is oil and gas fracking. We urge you to support legislation to ban fracking today."

- Following recent warnings aimed at energy companies against the impending threat of cyber attack, the industrial control systems of hundreds of European and US energy companies have been infected by a sophisticated cyber weapon operated by a state-backed group with apparent ties to Russia, according to leading US online security group, Symantec. The malware known as “Energetic Bear” allows it operators to monitor energy consumption in real time, or to cripple physical systems such as power plants and gas pipelines. The organization behind the attack is believed to have compromised the computer systems of more than 1,000 organizations in 84 countries in a campaign spanning 18 months.

- Activist Tim DeChristopher appeared at a Washington, DC rally against fracked gas exports on Sunday. DeChristopher had previously served federal prison time for using false bids to disrupt a federal auction of oil & gas leases. Upon his release, the rules of his probation prevented him from participating in “social justice” organizations, jobs, or activities. This appearance likely means that his probation has ended and he now has a free hand to assume a leadership role in the environmentalist movement.

- The Athens County Commissioners have agreed to write a letter to the U.S. Environmental Protection Agency urging them to review and perhaps take over Ohio’s oil and gas regulatory primacy from the Ohio Department of Natural Resources. The board of commissioners voted unanimously to send the letter after meeting with members of the Athens County Fracking Action Network, an anti-fracking group that has been highly critical of how ODNR regulates fracking activity in the state.

- Ohio activists are concerns about plans to build a facility on the Ohio River that would allow barging of fracking waste water.

- A new study by two Alberta First Nations and University of Manitoba scientists says there is a link between oilsands pollutants and higher levels of heavy metals in wildlife, and higher cancer rates in residents.

- The Sierra Club is planning a massive rally at the July 31 Pittsburgh EPA hearing on carbon emissions. Chapters from multiple states will send contingencies, and the President of the Sierra Club will speak.

- A fire at a fracking well site in Ohio on June 28 is being cited by activists as a reason to change chemical disclosure laws. The fire at the Monroe County well site on June 28 spread to 20 nearby trucks on the drilling pad, and required additional firefighters from six counties to contain it.

---

**Agribusiness**

- Severe weekend storms damage farms in western North Dakota and cause widespread crop damage. High winds and hail associated with severe storms that moved across North Dakota during the weekend of July 5 heavily damaged crops, including barley, soybeans, and corn as well as grain bins and farm buildings in the western portion of the State.

- On July 10, 2014 Ben & Jerry’s co-founder Jerry Greenfield along with some members of Congress and pro-GE labeling advocacy groups protested a House bill that has been
proposed that would restrict states from passing GMO labeling legislation. As part of the protest, a petition with over 500,000 signatures was delivered to Congress against the proposed bill. The story has been circulating widely on social media, and two examples have been included in the supplemental report.

- On July 10, 2014, The Huffington Post published a story about Congressional hearings this week in the House Agriculture Committee. According to the article, those involved in the hearings agreed that “People who oppose GMOs or want them labeled so that consumers can know what they’re eating are alarmists who thrive on fear and ignorance.” Some groups on social media have already responded with outrage at the report. One example of a tweet from Babes Against Biotech has been included in the supplemental section of the report.

- An article on mychamplainvalley.com from July 7, 2014 reports that the Vermont Attorney General’s Office has announced the team that will take on the lawsuit brought against the state by the GMA. Assistant Attorney General Megan Shafritz has been named as the lead attorney on the case. Other members of the AG office will be part of the team, as well as Lawrence Robbins of the DC law firm Robbins, Russell, Engle, Orseck, Untereiner & Sauber LLP. He will be paid about $1.465 million for his work on the case, which does not include work if the suit goes to an appeals court.

- The Agriculture Department is looking for White House approval of new poultry inspection rules that would allow processors to speed up production and direct USDA inspectors to devote more time to preventing meat contamination. Approval by the White House budget office would be one of the last steps before the proposal becomes official policy. Opponents to the proposal argue that this “essentially privatizes poultry inspections,” letting companies largely perform the work that was done by USDA inspectors.

- Many activist and advocacy groups including Landowners’ Alliance representing small-scale farmers participated in demonstrations in 16 UK cities on July 12, 2014 in protest of the Transatlantic Trade and Investment Partnership (TTIP). Opponents of the agreement say that it could threaten EU agriculture, being worth up to £100bn a year to the European Union. This comes amidst ongoing opposition from grassroots groups in the US and EU to this and other similar agreements.

- Agriculture Secretary Tom Vilsack said he has been so impressed by Nestlé’s barcode labeling system that he believes putting information about genetically modified ingredients in the same manner on food labels could resolve the issue of labeling foods that contain GMO ingredients.

- Triple Pundit reported that two advocacy organizations have announced that they will file motion to intervene in the lawsuit against Vermont by national food manufacturers, which includes the GMA. In particular, the Vermont Public Interest Group (VPIRG), one of the largest consumer and environmental groups in the state, will file a motion to intervene in the lawsuit filed by the GMA et al. The VPIRG played an instrumental role in passing the GMO labeling law in the first place, and also has a strong interest in seeing the initiative take effect, said Paul Burns, VPIRG executive director.

- Green Is The New Red, an independent news source, reported that a kickstarter campaign called “Drone on the Farm” is now fully funded. The project’s goal is to investigate farms belonging to the food industry using photography equipment, including thermal imagery. The article claims these drones can get around strict “Ag-gag” laws to expose the food industry.
Insurance

- As the Department of Health and Human Services' Office for Civil Rights prepares for a change in its top leadership, information security leaders are watching to see whether the strategies of the HIPAA enforcement agency might shift as well.

- Sorting through the privacy issues involved when giving patients access to their healthcare records via a Web portal is a challenging task. Differing state privacy laws and a lack of technology standards are among the factors that make patient portals complex to manage.

- In the wake of the HHS Office for Civil Rights recently issuing its largest HIPAA enforcement action to date - a $4.8 million settlement with New York-Presbyterian Hospital and Columbia University for the same 2011 data breach - healthcare entities and their business associates more than ever need to be ready for potentially intense regulatory scrutiny.

- Concerns that nationwide electronic health record adoption could lead to widespread fraudulent coding and billing practices that result in higher health care spending are unfounded, according to a study from the University of Michigan School of Information and the Harvard School of Public Health.

- Several Blue Shield of California spreadsheet reports inadvertently containing the Social Security numbers of 18,000 physicians and other healthcare providers were released 10 times by the state's Department of Managed Health Care.

- St. Vincent Breast Center in Indianapolis has notified 63,000 individuals that a clerical error led to the mailing of letters containing personal health information to the wrong recipients. The letters were sent to former patients of Indianapolis Breast Center, P.C. and Solis Women's Health Breast Imaging Specialists, both of which were closing their practices. The letters were to inform the patients that St. Vincent was available to provide care or to welcome those patients who had previously scheduled healthcare services.

- Birmingham city centre - dubbed Britain's whiplash fraud capital by SmartWitness - has the highest car insurance premiums in the whole of the UK, according to new research. SmartWitness managing director Simon Marsh said: "Part of the reason for the sharp increase for the car insurance premiums is that Birmingham has become the capital of whiplash claims in the UK."

Pharmaceutical

- Allergan, which is currently being pursued by Valeant Pharmaceuticals International Inc. in a hostile bid, will shelve unpromising pipeline drugs and overhaul management incentives, two people with knowledge of the matter said last week. A broad restructuring plan set to be outlined during Allergan's earnings announcement later this month will also involve company wide cost cuts, including some legacy expenses, said the people, who asked not to be identified because the effort isn't yet public. Management compensation will be more closely tied to achieving higher forecasts.

- Senators Amy Klobuchar and John McCain introduced legislation Tuesday that would allow people to import personal pharmaceutical drugs from Canada. The Safe and Affordable Drugs from Canada Act allows individuals to import cheaper drugs in the same dosage, form and potency as drugs in the United States. Chances of this legislation passing in the current session are slim, sources say.

- Nigeria's medicines regulatory authority has started enforcing a requirement for antimalarial and antibiotic drugs to deploy a text message-based authentication system. The MAS (message authentication system) involves placing a code on the medicine
pack that can be texted by any of the 100m Nigerian cell phone users to an associated phone number in order to verify the authenticity of a pack of medicines. Within a short time, their cell phone will receive a text message that indicates whether the code sent is genuine or bogus.

- More than 70,000 counterfeit products have been intercepted during a joint customs operation (JCO) in Europe codenamed ERMIS. JCO ERMIS was carried out by the Greek Customs Administration and the European Anti-Fraud Office (OLAF), and also involved customs experts from the EU as well as Macedonia, Montenegro, Serbia and Turkey. The operation took place in March and focused on identifying fake goods shipped through postal and courier traffic. The seized goods varied from mobile phones, sunglasses and small vehicle parts, to medicines and pharmaceutical products.

Financial

Activism

- Activists launched a petition against a leading U.S. bank in response to the bank’s recent employee survey with questions related to employees’ identification with the LGBT community.

- Housing activists in Atlanta, GA held a protest on July 9th against a property management company in support of a local resident who is facing eviction from her apartment owned by the company.

- Housing activists in several cities delivered a letter and petitions to Attorney General Eric Holder to US Attorney offices around the country, demanding to know what’s become of the supposed $13 billion in relief for struggling homeowners announced last year in a settlement with a leading U.S. bank.

- Housing activists in Springfield, MA conducted an eviction blockade training on July 10th to prepare for defending a local resident’s home against an alleged eviction attempt by a Government Sponsored Enterprise for housing.

- Activists in Michigan are planning to march against the Governor, the Detroit Department of Water and Sewerage, and a leading U.S. bank branch in downtown Detroit on July 18th to end “International Human Water Rights Violations.”

- Housing activists launched a phone campaign against the nation’s two U.S. Government Sponsored Enterprises for housing to prevent the eviction of a local family in Chicago, IL.

- Housing activists held a rally on July 8th in Minneapolis, MN in support of a local resident who is facing eviction by a leading U.S. bank.

- Housing activists conducted a rally on July 11th in Detroit, MI to halt the removal of twelve families opposing their eviction from a new community development.

- Activists called on a leading U.S. retirement services organization to divest from a British multinational security services company that supplies security equipment and services for use at Israeli prisons, checkpoints and settlements in the West Bank.

- A Jewish activist organization conducted a ‘Boycott/Divest from Israeli Occupation BDS Day of Action’ event in Boston, MA on July 9th.

- Activists conducted an anti-Israeli occupation of Palestine protest on July 9th against an Israeli home carbonation product manufacturer in Philadelphia, PA.
A pro-gun “open carry” protests took place at several leading U.S. bank branches throughout the U.S. on July 11th.

Housing activists marched to a leading U.S. bank branch in downtown Minneapolis, MN on July 8th, demanding the bank negotiate a fair deal for a south Minneapolis homeowner, and, to pay a multi-billion dollar settlement it agreed to last fall with the Department of Justice to help struggling homeowners.

An Occupy group in San Francisco will host a “convergence” on September 20th at Justin Herman Plaza in San Francisco, CA. The purpose of the event is to promote various Occupy initiatives and network with supporters. Other activist groups, including Occupy Oakland, will also participate in the event.

Information Security Risk

- Hackers claimed to have targeted a regional U.S. bank in Glasgow, KY with repeated DDoS attacks.

- Hackers claimed to have launched DDoS attacks against several regional U.S. banks and issued several threatening statements forewarning of the impending “destruction” of the US banking infrastructure.

- A Tunisian hacker group threatened to hack the U.S. financial sector during one of its anti-U.S. campaigns, which began on July 5th. The group demanded the U.S. Government withdraw its soldiers from Islamic countries, or they will attack U.S. financial targets as well as “airport computers.”

- A hacker group threatened congressional lawmakers to back off over the CISA cyber security bill if they value the “sanctity of their loved ones” and themselves, or face consequences in the form of mass ground protests.

- Researchers identified a malicious automated network that targets Point-of-Sale software using infected computers from around the world. The underground bot army, using the project name “@-Brt,” is using thousands of peaceful and unsuspecting infected users to brute force Point-of-Sales systems in an attempt to steal login credentials.

- A prominent cyber threat actor published a target list of Israeli banks for a variety of anti-Israel cyber campaigns, and further issued a warning statement to financial institutions in the region.

- A hotel in Houston, TX said it suffered a six-month “malicious software attack” that could have exposed customer credit card information. The attack lasted from December 28th to June 20th. The U.S. Secret Service notified the hotel of the attack on June 10th.

- A hacktivist collective launched multiple DDoS attacks against major banks and insurance companies in Norway. The attacks were detected and made public the morning of June 8th after Norway’s largest financial services group announced their website was partially down because of junk traffic affecting their systems, and customers experienced difficulties logging in.

- A survey conducted by a U.S. cyber security firm showed that 64% of UK IT decision-makers expect their organization to be the target of a cyber-attack within the next 12 months, and are uncertain about their ability to detect it. Reportedly, 49% of respondents said they did not even know if they had been compromised already. Also, 32% of respondents confirmed their business was hit by a cyber-attack during the past year, but confirmed that there are blind spots on enterprise endpoints. A full 61% of respondents rated their ability to detect suspicious behavior in advance of an attack as no better than average.

- Researchers discovered new strains of the malevolent Zeus malware using the
Windows 'PIF' file extension to steal information from compromised computer systems. These are believed to be an evolution of the coding used in previous Zeus variants. The emerging variants are being used in new low-volume email campaigns that target users' financial data. These strains of the banking Trojan have been seen to "persistently evolve and adapt their methods to implement information stealing procedures," and are believed to be a direct evolution of a previous variant called "Zberp." The Zberp Trojan, believed to have been assembled from the source code of Zeus and Carberp, allows cybercriminals to lift information from compromised computers including names, IP, data submitted in HTTP forms and FTP/POP accounts. The emails used by Zeus PIF often hold subjects used to lure a target to run a file from a URL and according to the team are of good quality; containing no spelling mistakes and convincing imagery.

- Researchers said mobile banking and mobile payment malware rose in the month of June, as the number of infected mobile devices worldwide, as well as the number of malware variants targeting the Android platform, increased at a high speed.

- Researchers said source code for an impressively small but capable malware program that targets online bank accounts has been leaked. The program, known as "Tinba" or "Zusy," was discovered around mid-2012 and infected tens of thousands of computers in Turkey. It is notable for having a very small code base -- just 20K -- but capabilities similar to malware much larger in size.

- Researchers said cybercriminals began taking steps to resurrect the Gameover ZeuS botnet, a complex crime machine that has been blamed for the theft more than $100 million from banks, businesses and consumers worldwide. The revival attempt comes roughly five weeks after the FBI joined several nations, researchers and security firms in a global and thus far successful effort to eradicate it.

**Legal, Litigation, Regulatory Risk**

- The U.S. Justice Department last week announced the arrest of a Russian hacker accused of running a network of online crime shops that sold credit and debit card data stolen in breaches at restaurants and retailers throughout the United States. The government alleges that the hacker known in the underground as “nCux” and “Bulba” was Roman Seleznev, a 30-year-old Russian citizen who was recently arrested by the U.S. Secret Service.

- Wall Street executives told a Senate Banking Committee on July 8th that SEC rules for a national market system has created a technology arms race that risks destabilizing U.S. stock markets because the regulations intend to promote competition among the exchanges and thus contribute to high-speeding trading risks. The committee also received calls to simplify the pricing model used by exchanges as the so-called “maker-taker” model pays rebates to traders who stand ready to buy or sell shares as needed, while charging those on the other side of the transaction. Exchanges profit off the difference between those fees.

- A federal judge denied a leading U.S bank’s latest bid to end a lawsuit brought by the Los Angeles city government accusing the bank of discriminatory lending that led to a wave of foreclosures among minority borrowers.

- Police in Greece made two arrests in connection with a little-known spamming botnet called “Lecpetex,” which used hacked computers to mine the Litecoin virtual currency. As many as 50,000 popular social media accounts were affected and as many as 250,000 computers worldwide, primarily in Greece, Poland, Norway, India, Portugal and the U.S.

- The FBI said a Romanian (Iulian Schiopu) has been sentenced to 45 months in prison for his role in a phishing scheme that netted thousands of credit and debit card numbers from U.S. financial institution customers. The scheme involved sending e-mails to customers purporting to come from various financial institutions, authorities say.
Schiopu, along with co-conspirators, used and shared a number of e-mail messages containing credit or debit card numbers, expiration dates, CVV codes, PIN numbers and other personal identification information, such as names, addresses, telephone numbers, dates of birth and Social Security numbers, prosecutors say. The co-conspirators then used the information to access bank accounts and lines of credit to withdraw funds without authorization, often from ATMs in Romania.

- An international law enforcement operation struck a major blow against the gang behind Shylock, one of the world's most dangerous financial Trojans. The takedown, which was led by the UK National Crime Agency, resulted in the seizure of a command and control (C&C) servers, in addition to domains that Shylock uses for communication between infected computers.

**Operational Risk**

- Two of the world's largest ATM makers formed a new organization and initiated an industry-wide effort to combat ATM-based crime. According to the announcement, plans for the association include compiling information on recognized and potential attack scenarios on ATMs that can be shared with industry groups to develop and implement counter-measures.

- Wall Street's biggest trade group has proposed a government-industry cyber war council to stave off terrorist attacks that could trigger financial panic by temporarily wiping out account balances. The proposal by the Securities Industry and Financial Market Association (SIFMA) called for a committee of executives and deputy-level representatives from at least eight U.S. agencies including the Treasury Department, the National Security Agency and the Department of Homeland Security, all led by a senior White House official.

**Reputational Risk**

- A post published last week at a popular anti-Wall Street blog claimed that a leading U.S bank attempted to foreclose on the author’s family home although they never missed a mortgage payment.

- A post made at a popular investor forum claimed that until the "beefed up" version of Rule 3370 becomes effective, U.S. MMs are "legally" processing orders made by naked short selling known as "cell boxing" out of Canada and other offshore locations even though they and the clearing firms involved knew by history that these shares were in no way going to be delivered. Further, this gaping loophole allows a US post-trade financial services company, which is basically the 11,000 b/ds and banks that’s referred to as "Wall Street", to borrow shares from those investors naive enough to hold these shares in "street name" at their brokerage firm. This amounts to about 95% of us."

- An article published last week criticized the Securities Industry and Financial Markets Association (SIFMA) for being Wall Street's largest lobbying group and leading a push to formally merge Wall Street with U.S. Government intelligence agencies. The article claimed that a merger between Wall Street and the U.S. intelligence community, "two of the most powerful and out of control segments of American society," is "fascism," and the "worst idea in the history of horrible ideas."

- An article published last week said Attorney General Eric Holder has formally refused to meet with the CEO of a leading U.S. bank as talks to resolve probes into shoddy mortgage securities sold by the bank and its units remain at a standstill.

**Global Intelligence**
Brazil

- On 7/8/2014 Pocket Lint reported that Samsung's factory near Sao Paolo was invaded late Sunday night and its workers were held hostage as the criminals made off with BRL $36 million worth of gadgets. More than 40,000 products were stolen.

China

- On 7/11/2014, a Chinese news outlet reports the number of recent government websites experienced malicious attacks increase by five times comparing to the number of last year.

- On 7/10/2014, a Chinese news outlet reports 360 Security Team discloses additional information regarding the Android security vulnerability that could be exploited by malicious application to initiate unauthorized phone calls and interrupt user's phone call.

- On 7/9/2014, a Chinese news outlet reports several Chinese sites experienced DDoS attack from unknown source. The sites mentioned in the article are AcFun.com (video stream site), Wooyun.org (security vulnerabilities news outlet), and Guokr.com (technology news outlet).

- On 7/8/2014, a security news outlet reports 360, a Chinese information security company claimed to have discovered a new technique of attack that is stealthier and better than the Oldboot and Bootkit attack. 360 claimed that the new technique allowed the hacker to do anything in the the mobile device.

- On 7/7/2014, a Chinese news outlet reports a ransomware capable of locking mobile devices current targeting torrent user by disguising as Torrent download mobile application. The ransomware has current locked nearly 60,000 mobile devices.

- On 7/7/3024, a Chinese news outlet reports the some android application provided by several Chinese Android application stores like Myapk.com and 7xz.com contain security vulnerabilities that could be exploited to push out advertisement, charging fee without user consent and stealing user information.

- On 7/5/2014, a Chinese news outlet reports a security vulnerability on devices with Android 3.1 and above, disclosure user's location while the device is in Preffered Network Offload mode.

- Samsung is facing accusations that one of its China suppliers hired children to meet production targets during a period high demand from the company. The plant in question is Shinyang Electronics located in Dongguan, Guangdong province. Samsung parties stated on Thursday that they were "urgently' looking into the allegations.

European Union

- On 7/3/2014 the Logan Reporter reported that Google has started removing search results for certain queries in compliance with the EU's ruling on the "right to be forgotten." The landmark legislation was upheld by the European Court of Justice on 5/13/2014 with regulators granting citizens in 28 EU member states the right to petition Google to remove links to sites containing information that they deemed 'inadequate, irrelevant or no longer relevant.'"

France

- On 7/7/2014 Telecompaper reported that IBM France has announced that it plans to hire 1,000 workers over the next two week to four years at the facility it opened last year in Lille, 300 more than previously announced.

Germany
• The committee of the German parliament (Bundestag) tasked with the investigation into foreign clandestine operations which might target German citizens and institutions is considering to use old-fashioned typewriters for internal communication to safeguard internal communication.

• German public broadcasting network NDR produced a documentary regarding hacking attacks aimed the Internet of Things. The documentary contains statements by Jörg Handwerg, speaker for professional pilot association Cockpit, who claims that computer systems on commercial airplanes are not sufficiently protected against hacking attacks, e.g. the autopilot function was vulnerable during an internal demonstration. Ships would be vulnerable as well.

Israel

• On 7/9/2014 Relocation Jobs reported that a strike planned for Tuesday by Israel’s main public labor union has been called off because of the escalating conflict between Israel and the Palestinian.

Japan

• On 7/10/2014 the Japan Times reported that public-sector workers in the UK walked out on 7/10/2014 to protest pay, pension and job cuts, closing schools, courts and libraries across the country. Government employees belong to United, Unison and the GMB labor groups joined members of the National Union of Teachers, the Fire Brigades Union and the Public and Commercial Services union in a day of action focused on below-inflation pay rises for workers across the public sector.

Malaysia:

• On 7/3/2014, a Malaysian human right activist, Charles Hector posted on a labor right blog regarding the link between cancer and electronic industry. He also used the example of the Samsung case regarding two Samsung employees developed leukemia due to toxic chemical.

• On 7/8/2014, a Malaysian news outlet reports Union Network International-Malaysian Liaison Council president responded to Malaysia Airline executive’s statement regarding the labor union is main obstacle to the company for being profitable. Union Network International-Malaysian Liaison Council president claimed that Malaysia Airlines System Employees Union (Maseu) is always open minded and supported any change which did not jeopardize any party, do not blame the union for the company losses.

• On 7/11/2014, a Malaysian news outlet report the Home Minister calls on Malaysian to condemn Israel for attacking Palestinians in Gaza.

New Zealand

• On 7/14/2014 IT Wire reported a New Zealand Internet Service Provider Slingshot is seriously differentiating itself from its competitors by offering customers the ability to watch Netflix, or BBC iPlayer, or any other localized Internet sites, without restriction and allowing its customers to option to pay for the services with bitcoins.

North America

• On 7/1/2014 JD Supra, a legal forum, reported that a federal appellate court upheld the dismissal of a lawsuit alleging that a Dairy Queen franchisee failed to reasonably accommodate a blind employee under the Americans with Disabilities Act (ADA), in Bunn v. Khoury Enterprises, Inc. The court held that Dairy Queen met its obligations under the ADA to provide a reasonable accommodation, even if it was not the accommodation preferred by the employee and even if Dairy Queen did not engage him in discussion regarding his preferred accommodations.
On 7/9/2014 Bidness ETC reported that Microsoft has decided to comply with European Union regulations over the "right to be forgotten" by introducing request forms for users who want removal of obsolete or personal information from Bing's search results.

On 7/8/2014 Pando Daily reported that an apparent crazy person filed a fake legal document demanding Judge Lucy Koh be removed from the case due to her own "Obama conflict." According to the article, the attorney listed as filing the motion knew nothing about. A copy of the filing was included in the article.

On 7/8/2014 the Albany Business Review reported that IBM is expected to sell its chip manufacturing business as its chip manufacturing business and GlobalFoundries is a top contender to make the purchase to gain access to intellectual property and skilled employees. An announcement is expected this week regarding GlobalFoundries' purchase of IBM's chip manufacturing business.

On 7/7/2014 Workforce reported that the EEOC had filed suit on behalf of a diabetic employee who, without permission, took a bag of chips off the shelf to stabilize her blood sugar level during a hypoglycemic attack. Walgreens considered it shoplifting and fired the employee. The EEOC considered the termination a failure to reasonably accommodate the employee's disability and filed suit. Last week, Walgreens settled the lawsuit, agreeing to pay the ex-employee $180,000, in addition to agreement to implement revised policies and training.

On 7/7/2014 Times Union reported that Infosys Ltd joined a federal lawsuit alleging Infosys Ltd, the global staffing firm that ran Harley-Davidson's tech support, discriminated against American workers in part by replacing them with temporary workers from South Asia. According to the article, amid the calls for expanding the nation's H-1B visa program, there is growing push back from Americans who argue the program has been hijacked by staffing companies that import cheaper, lower level workers to replace more expensive U.S. employees - or keep them from getting hired in the first place.

Anti-Israeli protestors have targeted western media outlets News Corporation and Sky News. On Thursday July 10th, protestors in New York City marched from the United Nations building to the parent of Fox News in an attempt to address outrage over the media’s coverage of the conflict.

Vietnam

On 7/9/2014 Vietnam+ reported that in the second quarter of this year, the demand for IT engineers surged as Japan moved some of its software projects from China to Vietnam. In the past few months, enterprises such as FPT Software, Global Cybersoft and Fujinet recruited hundreds of information technology (IT) engineers. Some even asked for 50-100 engineers at once. Global Cybersoft said it needed more than 150 engineers last month and this. For the whole year, it's estimated labor needs for engineers and apprentices is over 500. FPT Software stated that it would require 900 engineers this year to expand its business for Japanese and North American markets.

On 7/9/2014 Lao Dong News reported that Samsung Electronics VN always pays union dues fully. According to the article, Samsung not only pays for its portion of the union dues but it also pays the portion of union dues the workers are responsible to pay for themselves (1% of the workers' monthly salary).

On 7/6/2014 ChaoBuoiSang.Net reported that Vietnam is expected to attract Foreign Direct Investments (FDI) worth $8 Billion USD into its Industrial Zones (IPs) and $2 billion USD into Economic Zones (EZs) this year.

On 7/5/2014 Vietnam.Net reported that the number of technology groups have set up their factories in Vietnam, giving many reason to believe that Vietnam is destined to become the world's major electronics production base. The Ho Chi Minh City
High-technology Park has reportedly attracted 30 hi-tech projects over the four years since it began operations. Investors in the park include Intel, Nidec, and Datalogic.

### Legal and Regulations

**Financial Services**

- Beginning in October of 2015, merchants, card issuers, and payment processors must comply with new technical requirements (known as the EMV standard) for debit and credit cards and the accompanying point of sale (POS) infrastructure, or risk being held responsible for the cost of fraudulent in-person transactions. The United States is the last major world economy to adopt these new standards. Named after its original creators (Europay, MasterCard, and Visa), the EMV standard requires smart chip technology to be embedded in payment cards, and also requires new POS devices capable of utilizing the capabilities of the chip technology. Compliance with the new standard is not mandated by the card association operating rules. However, merchants that don't have POS equipment that meets the new standard by October 2015 (October 2017 for automated fuel dispensers) will assume liability for many fraudulent purchases. Don't wait to start planning an equipment migration. Now is the time to begin developing a strategy for implementation of the EMV standard. POS equipment upgrades can be expensive and time consuming.