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

- BP and ExxonMobil have both ordered staff to leave Iraq, and China is considering pulling some of its 10,000 workers from projects following the turmoil caused by jihadist rebel group ISIS, which has rocked the country and threatened security. Exxon is plucking 20 percent of its staff, mostly foreigners, from Iraq fearing the Sunni rebel group ISIS, a breakaway Al-Qaeda group, could target oilfields and refineries in their terror sweep. An official from Iraq’s state-run South Oil Company confirmed this on Wednesday. BP has shipped out all non-essential employees from the Rumaila field in the south and Exxon has been evacuating staff from the West Qurna 1, also in the south.

Agribusiness

- Farmers For Action in the UK are planning further protests as part of their major campaign against falling beef prices. The farm lobby group targeted ABP’s Shrewsbury meat processing plant earlier this month amid unconfirmed claims that company had been processing Polish beef in the abattoir.

Insurance/Healthcare

- Social engineering threats are a reality that the healthcare industry is beginning to prioritize. Franciscan Health System of Tacoma, Wash. recently dealt with an email phishing attack and part of taking phishing attacks seriously is educating users.

Financial Services

- Researchers said attackers are targeting vulnerabilities in major Web browsers to compromise cloud-based point-of-sale (PoS) systems. The malware, called POSCLOUD, targets cloud-based PoS software commonly used by grocery stores, retailers, and other small businesses. Unlike most PoS malware, POSCLOUD doesn’t bother with RAM scraping to intercept payment card information before the system gets a chance to encrypt the data. Instead, the malware relies on keylogging and stealth screenshots to steal personal information and financial data, which are then sold on underground forums to identity thieves.

Global Intelligence

- Tens of thousands of email passwords disclosed: Files with credentials for more than 60,000 email accounts were stored on servers in southern Europe. The data sets contain email accounts, open passwords, and server names. Many victims seem to be German consumers, businesses, and government organizations. It is suspected that the data was collected with malware and phishing emails.

Legal and Regulations

- The U.S. Food and Drug Administration (FDA) released today two highly anticipated draft guidance documents:
  1. Internet/Social Media Platforms with Character Space Limitations—Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices; and
  2. Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices.

These guidance documents are in response to significant industry pressure for clarity on social media promotion.
Hundreds of protestors gathered Tuesday in the PA Capitol Rotunda and called on Gov. Tom Corbett to impose a severance tax on Marcellus shale drillers to raise revenue instead of leasing forests and parks for natural gas development.

The Utah Tar Sands Week of Action will be held July 18 – 29. Organizers are attempting to tap into nationalist sentiment by promoting the fact that the mine being protested is will be opened by a Canadian firm.

Rising Tide North America is planning its Continental Gathering for August 22-24, near Whitesburg, KY. The conference will focus on mountaintop removal mining, although it will likely touch on other hot-button issues, such as coal, fracking, and energy trains.

The Sea Shepherd Conservation Society is expanding its use of drones and livestream video in its actions. The group began experimenting with drones in previous seasons, but now appears to be relying on drone surveillance tactics to inform and allocate forces.

BP and ExxonMobil have both ordered staff to leave Iraq, and China is considering pulling some of its 10,000 workers from projects following the turmoil caused by jihadist rebel group ISIS, which has rocked the country and threatened security. Exxon is plucking 20 percent of its staff, mostly foreigners, from Iraq fearing the Sunni rebel group ISIS, a breakaway Al-Qaeda group, could target oilfields and refineries in their terror sweep. An official from Iraq’s state-run South Oil Company confirmed this on Wednesday. BP has shipped out all non-essential employees from the Rumaila field in the south and Exxon has been evacuating staff from the West Qurna 1, also in the south.

BP and ExxonMobil have both ordered staff to leave Iraq, and China is considering pulling some of its 10,000 workers from projects following the turmoil caused by jihadist rebel group ISIS, which has rocked the country and threatened security. Exxon is plucking 20 percent of its staff, mostly foreigners, from Iraq fearing the Sunni rebel group ISIS, a breakaway Al-Qaeda group, could target oilfields and refineries in their terror sweep. An official from Iraq’s state-run South Oil Company confirmed this on Wednesday. BP has shipped out all non-essential employees from the Rumaila field in the south and Exxon has been evacuating staff from the West Qurna 1, also in the south.

BP and ExxonMobil have both ordered staff to leave Iraq, and China is considering pulling some of its 10,000 workers from projects following the turmoil caused by jihadist rebel group ISIS, which has rocked the country and threatened security. Exxon is plucking 20 percent of its staff, mostly foreigners, from Iraq fearing the Sunni rebel group ISIS, a breakaway Al-Qaeda group, could target oilfields and refineries in their terror sweep. An official from Iraq’s state-run South Oil Company confirmed this on Wednesday. BP has shipped out all non-essential employees from the Rumaila field in the south and Exxon has been evacuating staff from the West Qurna 1, also in the south.

A Middle East-based group of hackers issued a threat warning of cyber attacks against oil, gas and energy companies in the Middle East. The threat, made by Anonymous, a politically motivated group of hacktivists, states that they are planning to attack before, during, and after June 20, 2014. This is due to Anonymous disagreeing with the US dollar being used as the currency to buy and sell oil.

On June 9, Al-Qaeda attacked power lines in Yemen’s central province of Marib, and sources report they knocked out the entire national power grid. “This is the first case where a terrorist attack on the power grid has blacked out an entire nation,” said Peter Vincent Pry, who once was staff director of the congressionally mandated EMP commission, which determined the impact of an electromagnetic pulse event on the life-sustaining critical infrastructures in the United States that rely completely on the vulnerable national grid system.

On June 17, a major natural gas pipeline exploded in Central Ukraine. The day prior, the Russian energy company Gazprom said that it was cutting off supplies to Ukraine in a dispute over pricing, and officials immediately labeled it a possible act of sabotage. Utility officials said that natural gas deliveries were not interrupted and that supplies to Ukrainian customers and other European countries were flowing through alternative pipes.

A lawsuit from the American Bird Conservancy was expected to be filed Thursday in federal court, the conservation group says it’s suing the Obama administration over a new federal rule that allows wind-energy companies to seek approval to kill or injure eagles for 30 years. The group argues that the rule, which extended by 25 years the length of time companies may kill or injure eagles without fear of prosecution, is illegal because the U.S. Fish and Wildlife Service failed to evaluate the consequences and ensure it would not damage eagle populations. The Obama administration classified the rule as an administrative change, excluding it from a full environmental review. "In the
government's rush to expand wind energy, shortcuts were taken in implementing this rule that should not have been allowed,” said Michael Hutchins, the national co-ordinator of the conservancy’s wind energy program.

- Opponents of Enbridge’s Northern Gateway project spent the day after its conditional approval from Ottawa waging war on several fronts, Taking Direct action, using civil disobedience, legal action, and persuasion to further the message that the $7.9-billion pipeline should not be built.

- Russia’s Ecodefense, the leading anti-nuclear power organization in the country, was branded a “foreign agent” by the Russian government. Under Russian law adopted recently, non-profit organizations that fail to register as a “foreign agent” but are found to be one can be subject to large fines and dissolution of the organization. While part of the international NIRS/WISE network, Ecodefense was founded in Russia, is based in Russia, and has focused on issues affecting Russia. It has, for those reasons, refused to register as a “foreign agent,” which in Russia is tantamount to an admission that the organization is controlled from abroad and effectively is undertaking espionage activities on behalf of other nations—neither of which is true in the case of Ecodefense.

Agribusiness

- Wheat rose for a second day on concern that rain from Oklahoma to Kansas may delay harvesting and cause crop quality to deteriorate in the U.S., the world’s biggest exporter.

- Agriculture Secretary Tom Vilsack announced that the United States and Hong Kong have agreed on new terms and conditions that pave the way for expanded exports of U.S. beef and beef products to Hong Kong.

- Ben & Jerry’s is not only changing one of the names of its ice cream flavors to highlight the GMO food fight, it will also donate $1 per ice cream purchase from its Burlington and Waterbury, Vt., shops to the GMO legal defense fund.

- Over-application of nitrogen fertilizer results in a larger than previously estimated release of nitrous oxide, one of three major greenhouse gases, says research by Michigan State University appearing in the Proceedings of the National Academy of Sciences.

- Farmers For Action in the UK are planning further protests as part of their major campaign against falling beef prices. The farm lobby group targeted ABP’s Shrewsbury meat processing plant earlier this month amid unconfirmed claims that company had been processing Polish beef in the abattoir.

- ePure used its first state of the industry report to call for long-term policies to boost investor confidence, binding targets for biofuel in transport and action to stop cheap imports flooding into Europe.

- European farm ministers have failed to agree on measures to ease the superlevy fine for overproduction in the last year of milk quotas.

- U.S. veterinarians are warning that outbreaks of a deadly pig virus will climb this autumn after a summertime hiatus, likely killing another 2.5 million pigs over the next 12 months and amplifying an increase in pork prices.

- Organic foods chain, Whole Foods, is facing a class-action lawsuit over “all-natural” claims. A judge from the California U.S District has allowed the claims to go forward.
Scores of blunders sees Norfolk councils breach data laws over confidential information

NHS patient information in data breach by Diagnostic Health

The Workgroup for Electronic Data Interchange (WEDI) did a lot of work with the Office for Civil Rights (OCR) last summer in helping to educate healthcare organizations on upcoming HIPAA Omnibus Rule regulations.

Though sometimes the goals of the HIPAA Privacy Rule can get lost in data breach and monetary penalty news, ensuring that patient data is both properly protected and accessible should be a consistent focus for the healthcare industry. Balancing these two functions and properly disclosing patient data in the right situations is no afterthought for healthcare organizations.

An acrimonious dispute between a community health center and its former IT director has evolved into a breach investigation by Connecticut's attorney general. The case involves Middletown-based Community Health Center, which operates 13 public clinics in the state, providing primary care services in medicine, dentistry and behavioral health, including specialized care services to patients with HIV/AIDS.

Advanced Care Hospitalists notifies patients of breach at billing vendor

Patients whose personal information is misused in the new medical records data-sharing scheme should be able to sue the NHS, a new report suggests. People whose data is lost or “irresponsibly used” under the care data initiative should be able to claim compensation through the NHS Litigation Authority

Healthcare entities should not write business associate agreements with provisions that go beyond HIPAA privacy and security regulations, says attorney Gerry Hinkley, who discusses HIPAA Omnibus Rule compliance issues.

Assuming a disclosure is not permitted in the HIPAA Privacy Rule, a healthcare organization must limit patient data uses and disclosures to only those that are authorized.

Social engineering threats are a reality that the healthcare industry is beginning to prioritize. Franciscan Health System of Tacoma, Wash. recently dealt with an email phishing attack and part of taking phishing attacks seriously is educating users.

Rady Children’s Hospital of San Diego is sending out letters to 14,121 patients and their families to notify them of a human error data breach that occurred on June 6 when patient data went mistakenly sent out to job applicants.

Even though the storms have passed, homeowners are still at risk, this time of scammers looking to solicit business to remove trees or repair roofs. Sometimes the companies are local and trustworthy, but oftentimes they’re from out of town and are providing fake information.

Former West Mansfield insurance agent Robert Horney, of Marysville, Ohio, was sentenced in Logan County Common Pleas Court to serve 60 days in jail, five years on community control and ordered to pay more than $21,000 in restitution for multiple fraud-related offenses, the Ohio Department of Insurance announced.

To help prevent data breaches involving business associates, healthcare organizations need to develop vendor management programs with razor-sharp requirements, says risk management expert Rocco Grillo.
Financial

Activism

- Protests against Tony Abbott’s financial budget will occur throughout Australia, including Sydney and Brisbane, on July 6th.

- Housing activists in Detroit, MI picketed outside the Ferndale Housing Commission Board meeting on June 18th in Ferndale, Michigan in support of a local housing voucher recipient who’s about to be evicted from her apartment.

- Activists launched a petition calling on a leading U.S. bank to provide adequate training to its call center employees.

- Activists conducted an anti-austerity demonstration on June 21st at Bedford Square in London, UK, denouncing the government and “bankers, lawyers, CEOs, new money, old money.”

- Housing activists held an anti-eviction themed block party event on June 21st and 22nd in Chicago, IL in support of the human right to housing.

- Housing activists in Detroit, MI urged supporters to call a government-sponsored mortgage association and demand the association let a local resident repurchase her foreclosed house.

- A housing activist group urged consumers to send emails to both Congress and the Director of the Federal Housing Finance Agency demanding they allow the two government-sponsored enterprises (GSE) for housing to reduce loan balances for underwater homeowners, increase multifamily apartment buildings financed by the GSEs, and ensure that they serve all credit worthy borrowers and provide funding for the National Housing Trust Fund.

- Occupy Wall Street hosted an assembly on June 20th at Union Square Park in NYC to “unveil its 99% strategy. The aim is to help rebuild the Occupy Movement by reconnecting and addressing the direct needs of the people, which are wages and housing.

Information Security Risk

- Hackers launched a cyber-attack against the servers and website of a leading Iraqi investment bank.

- Researchers uncovered a new banking Trojan called either Dyre or Dyreza which has the ability to bypass SSL protection for banking sessions by redirecting traffic through the attackers’ own domains. Dyreza uses a technique known as browser hooking to intercept traffic flowing between the victim’s machine and the target Web site. The malware arrives in users’ inboxes through spam messages, many of which will look like messages from a financial institution. The list of targeted organizations includes several international banks. Researchers said much of the activity from the Trojan so far is in the U.K.

- Researchers said attackers are targeting vulnerabilities in major Web browsers to compromise cloud-based point-of-sale (PoS) systems. The malware, called POSCLOUD, targets cloud-based PoS software commonly used by grocery stores, retailers, and other small businesses. Unlike most PoS malware, POSCLOUD doesn't bother with RAM scraping to intercept payment card information before the system gets a chance to encrypt the data. Instead, the malware relies on keylogging and stealth screenshots to steal personal information and financial data, which are then sold on
• Researchers identified a vulnerability which can allow attackers to disable Microsoft’s antimalware products by sending specifically crafted files to users via websites, email, or instant messaging applications. The vulnerability is located in the Microsoft Malware Protection Engine, which sits at the core of many Microsoft security products for desktops and servers including Microsoft Forefront Client Security, Microsoft System Center 2012 Endpoint Protection, the Microsoft Malicious Software Removal Tool, Microsoft Security Essentials, Windows Intune Endpoint Protection and Windows Defender, which comes pre-installed in Windows Vista and later. Microsoft fixed the vulnerability in Microsoft Malware Protection Engine 1.1.10701.0 released Tuesday. However if left unpatched, the vulnerability can be exploited to force the Microsoft Malware Protection Engine into a scan timeout, essentially leading to a denial-of-service vulnerability.

• Hackers claimed to have downed the website of an Israeli debt securities company.

• The Department of Homeland Security stated that the system that’s used to produce RFID-enabled identification cards—including permanent resident IDs—by the United States Citizenship and Immigration Service has a number of serious security issues. Among the issues is that nearly all of the workstations in the system were missing six years’ worth of Java patches and an Oracle database server was missing nearly two dozen patches.

• A British cyber-security firm said in an audacious and sophisticated attack, cybercriminals acting in late 2013 installed a malicious computer program on the servers of a large hedge fund, crippling its high-speed trading strategy and sending information about its trades to unknown offsite computers. Attackers went after the hedge fund’s trade order entry system, seeking to disrupt the fund’s trading strategy and to send details of the trades themselves outside of the firm. According to experts, the hack represents one of the most complex seen in a new wave of attacks designed to extract business strategy information from firms in a range of industries.

• A hacker claimed to have hacked a leading U.S. bank’s IVR (interactive response system) and gained unauthorized access to information.

• Researchers discovered a Google Play clone that can send text messages, signature certificates, and bank passwords to Gmail accounts. The attacker uses a dynamic DNS server with the Gmail SSL protocol in order to exfiltrate the collected data. Once started, the fake app, called “googl app stoy,” requests administrator privileges and, instead of an interface, launches error messages and informs the user that it has been deleted and that “googl app stoy” activity has stopped. Upon closer inspection, however, only its icon is removed, as the app is still active in the background and launches a set of five services. It is present in the list of apps currently running on the device and it cannot be removed or uninstalled. This is of particular importance because users have to launch it only once for it to become active and traces of suspicious activity can remain undetected, since the legitimate Google Play icon is still in place.

• A new report by a leading cybersecurity firm said while the United States, Japan and India were hit hardest by online banking malware in the first quarter of this year, Malaysia also showed up among the top 10 countries plagued by the malware. The overall number of online banking malware detected by the firm was approximately 116,000, an increase from 113,000 detections in the first quarter the year before. Research revealed that, at 23 percent, the U.S. accounted for the largest number of online banking malware detections followed by Japan (10 percent) and India (9 percent). But Malaysia showed up on par with Australia, France, Vietnam and Mexico.

Legal, Litigation, Regulatory Risk

• A senior U.S. Treasury official rejected calls to recapitalize the nation’s two government-
sponsored enterprises for housing, saying it would take at least 20 years to make sure they were adequately funded and that in the meantime taxpayers would be on the hook.

- The pricing model used by U.S. stock exchanges to attract liquidity came under fire last week, as a top Wall Street executive called for ending the practice and two U.S. senators raised concerns about the potential conflicts it creates. In a Senate hearing, an official from an international financial firm managing a global network of exchanges and clearing houses for financial and commodity markets expressed support for ending the "maker-taker" model used to reward brokers who make offers to buy or sell stocks on exchanges.

- A Housing and Urban Development secretary nominee urged lawmakers last week to move forward with efforts to shutter the nation's two government-sponsored enterprises for housing, saying that the current housing finance system is not serving Americans well.

**Operational Risk**

- In an effort to crack down on loans that violate state laws, New York state has created a database for banks to use to help identify untrustworthy lenders.

- An American stock exchange reported that a technical glitch halted trading in billions of euros worth of futures contracts tied to European money market rates Tuesday (June 17th) on a futures exchange based in New York City.

- A Dubai exchange glitch on June 15th showed an Abu Dhabi (UAE)-controlled private joint stock company had reduced its holding in the company to 14.32 percent from 18.85 percent. The website later updated the stake to 18.94 percent and blamed a "temporary system glitch" for the error. The company last week cut its ownership from 21.57 percent.

- The Hong Kong Monetary Authority conducted an emergency drill with 55 banks ahead of the Occupy Central movement's threat to blockade the streets of the business district. As bankers were testing their back-up plans, more than 300 campaigners for democracy set off from the business district for the first of seven days of marches aimed at rallying citizens of Hong Kong to vote in Occupy Central's "civil referendum" on electoral reform. Reportedly, "The drill assumed that due to unexpected events, the headquarters or other important operating sites of banks in Central as well as the HKMA's office, became inaccessible."

- An international online organization known for publishing secret information, news leaks, and classified media from anonymous sources released "the secret draft text for the Trade in Services Agreement (TISA) Financial Services Annex, which covers 50 countries and 68.2% of world trade in services." The website notes that in a "significant anti-transparency manuver" by the U.S. and EU, the Financial Services Annex draft has been classified to keep it secret not just during the negotiations but for five years after the TISA enters into force. Further, "the draft Financial Services Annex sets rules which would assist the expansion of financial multi-nationals – mainly headquartered in New York, London, Paris and Frankfurt – into other nations by preventing regulatory barriers. The leaked draft also shows that the US is particularly keen on boosting cross-border data flow, which would allow uninhibited exchange of personal and financial data."

**Reputational Risk**

- Activists published a post on a website associated with Occupy Wall Street, accusing a leading U.S. bank of employing a "social media trolling" spy team" to monitor political/activist groups.

- A major coastal city in Florida has sued several leading U.S. banks, accusing them of a pattern of discriminatory loan practices "since at least 2004" which sparked foreclosures
and violated the U.S. Fair Housing Act.

- An article published last week claimed that a leading U.S. bank “admitted to skimming off the top from retirees” as the bank paid a $32.4 million fine from the Financial Industry Regulatory Authority, which included $24.4 million in restitution to customers, and small business’ retirement accounts.

- An article published last week lamented that almost six years after the financial crisis, the nation’s largest banks finally face fines of around $12 billion each for their role in mortgage malfeasance. The article notes that in the context of the damage done and the bailout money poured into banks, the fines are miniscule and won’t even cover reparations in one or two blighted areas.

- An official from an American conservative non-profit think tank based in Washington, D.C. accused a leading U.S. bank of closing accounts of people with “Muslim names without assigning reason.”

Global Intelligence

China

- A Chinese news outlet reports that Chinese multinational consumer electronics and home appliances company Haier will cut another 10,000 employees from its workforce this year, according to company CEO Ruimin Zhang. Haier's increased utilization of smart unmanned manufacturing processes has lowered the need for manpower and manual labor.

- A Chinese news outlet reports Hong Kong Cilve Referendum online voting system experienced a hacker attacks and causes the referendum to be postponed for 7 days.

- A Foxconn laptop assembly plant in Chongqing is scheduled to close down by August. Allegedly, 800 angered workers have been on strike demanding compensation for lower-ranked employees. The three-day strike ended on the 19th when local government parties intervened in negotiations and plant officials promised to meet workers’ demands.

- A Chinese news outlet reports 57000 mobile devices infected a trojan that able to lock users' mobile devices for 24 hours.

- In a 6/20/2014 Youku video commented and shows that Facebook were experiencing a massive DDoS attack in 10 seconds. This as been included as supplemental URL.

- A Hong Kong news outlet reports Next Media official website experienced a hacker attacks.

- A Chinese news outlet report Anonymous may launch a large scale attack targeting Word Cup partners and sponsors. According to the article, an Anonymous member, AnonManifest has successfully invaded the Brazilian Ministry of Foreign Affairs database, obtains sensitive email access data, and launch DDoS attack.

- A Hong Kong news outlet reports an electronic voting system called "PopVote", which is going to be used in the 6.22 Civil Referendum in Hong Kong, experience a DDoS attack over the weekend.

Europe

- Tens of thousands of email passwords disclosed: Files with credentials for more than
60,000 email accounts were stored on servers in southern Europe. The data sets contain email accounts, open passwords, and server names. Many victims seem to be German consumers, businesses, and government organizations. It is suspected that the data was collected with malware and phishing emails.

Israel

- An Israeli media source, reported that the Economic Organizations Liaison Committee, chaired by Zvika Oren, and the Histadrut (General Federation of Labor in Israel) are due to sign a special collective agreement under which 3% of employees at a business with at least 100 employees must be handicapped. Regulations for smaller employees will be drawn up later.

North America

- 2014 ComputerWorld reported that the judge presiding over the Silicon Valley tech workers wage suppression class action expressed concerns that the $324 million settlement may not be a fair amount to the roughly 64,000 technology workers represented in the case.

- Valley Wag reported that ThoughtSpot, a start up company, is now offering up a $20,000 referral bonus. ThoughtSpot's CEO expressed to San Francisco Chronicle that the $20,000 bounty is actually less than the cut many recruiting companies take.

- A list of individuals interested in the auction of the 30,000 bitcoins confiscated from the Silk Road black marketplace has been leaked via email by the US Marshals Service (USMS), the US government agency confirmed. The US Marshals service is the agency that has been charged with conducting the auction of bitcoins that were originally seized by the FBI. The list details a diverse group of individuals and possible bidders representing members of the bitcoin community and the investment world.

- Forbes reported that there has been a recent explosion in state and local workplace pregnancy protections has dramatically increased the number of employers required to reasonably accommodate pregnant employees. Fourteen jurisdictions now impose such a duty, with many going far beyond federal requirements. The new laws have broader application than the ADA and FMLA, with some applying to employers with as few as 1-4 employees. Many also impose accommodation duties on employers with respect to pregnant employees that are more onerous than even the ADA with respect to disabled employees.

Malaysia

- A Malaysian news outlet report cases of dengue fever reported in Penang Island increased by 177% comparing to the same period of last year.

- A Malaysian news outlet reports HP and Seagate finalized investment and will be launching manufacturing plant in Penang.

- Malaysian human rights activist, Charles Hector highlighted the issue of immigrant workers being sent back to their country after participating in the ‘secret ballot’ for union recognition. Although he did not point the name of the companies but he encourage the unions to fight for this issue instead of keeping quiet on this issue.

- A Malaysian news outlet report the opposition political party, People Alliance guarantee to implement minimum wage of RM1100 if they are given a chance to rule the country.
• Times Union reported that U.K.’s Office for Security and Counterterrorism chief announced that U.K.’s electronic spy agency is legally allowed to track the online activities of millions of Britons who use U.S.-based platforms such as Facebook, Twitter and Google because data sent on those services is classed as "external" rather than "internal" communications because the companies' servers are based outside Britain.

Legal and Regulations

The U.S. Food and Drug Administration (FDA) released today two highly anticipated draft guidance documents:

1. Internet/Social Media Platforms with Character Space Limitations—Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices; and

2. Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices.

These guidance documents are in response to significant industry pressure for clarity on social media promotion.

Every company would be well advised scrutinize their marketing practices on an ongoing basis to ensure that they do not inadvertently expose the company to risks under the Lanham Act. Two US Supreme Court cases decided this term could result in a substantial increase in the number of Lanham Act claims brought under that statute alleging "unfair competition" resulting from product labeling and marketing practices that are alleged to be false or misleading.

- *Lexmark International, Inc. v. Static Control Components, Inc.*, No. 12-873, *slip op.* (March 25, 2014), in which the Supreme Court broadly construed the Lanham Act to permit lawsuits by all companies alleging injuries that were proximately caused by false or misleading advertising or promotion, even if the plaintiff was not a direct competitor of the defendant and suffered only "collateral damage."

- *Pom Wonderful LLC v. Coca-Cola Co.*, No. 12–761, *slip op.* (June 12, 2014), the Court’s second Lanham Act case of the term, in which it eliminated a potential safe harbor from Lanham Act claims for companies in regulated industries who complied fully with applicable regulations regarding the labeling and marketing of their products.

Telecommunications

Please be reminded of the upcoming due dates for the FCC Reports listed below:

- **Quarterly Section 63.10(c)(2) International Traffic and Revenue Report** - All carriers, including both resellers and facilities-based carriers, that are classified as dominant must file a quarterly report detailing traffic and revenue data for each service provided on those routes on which the carrier is classified as dominant. The report must be filed with the FCC by June 30, 2014.

- **Quarterly Section 63.10(c)(3) Quality of Service Report** - All carriers, including both resellers and facilities-based carriers, that are classified as dominant must provide information regarding the provisioning and maintenance of all basic network facilities and services procured from the carrier’s foreign carrier affiliate for those routes on which the carrier is classified as dominant. The report for the calendar quarter of January 1, 2014 through March 31, 2014 must be filed with the FCC by June 30, 2014.

- **Quarterly Section 63.10(c)(4) International Circuit Status Report** - Facilities-based carriers that are classified as dominant must report on the status of all circuits used to provide international service on those routes on which the carrier is classified as dominant. Information regarding activated or idle circuits must be reported on a facility-by-facility basis. The report for the calendar quarter of January 1, 2014 through March 31, 2014 must be filed with the FCC by June 30, 2014.
Quarterly Section 1.767 Submarine Cable Licensee Circuit Status and Provisioning and Maintenance Reports - Section 1.767 reports must be filed by submarine cable licensees that (i) are, or are affiliated with, carriers with market power in any of the submarine cable's WTO Member destination countries; and (ii) that have sought streamlined processing of a cable landing license, pursuant to section 1.767 of the Commission’s rules.

Filers must submit the following Provisioning and Maintenance and Circuit Status Reports:

- **Section 1.767 Provisioning and Maintenance Report** - The provisioning and maintenance report summarizes the provisioning and maintenance of all network facilities and services procured from the filer’s foreign carrier affiliate, in the destination market. The report must contain the following information: the types and volume or quantity of provisioned services and facilities; the time interval between order and delivery; and the number of outages and intervals between fault report and facility or service restoration.

- **Section 1.767 Circuit Status Report** - The circuit status report must be filed in the format set out in section 43.82 of the Commission’s rules and must report the status of all circuits used to provide international service in the destination markets. Activated or idle circuits must be reported on a facility-by-facility basis.

- The reports for the calendar quarter of January 1, 2014 through March 31, 2014 must be filed with the FCC by **June 30, 2014**