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

REGISTER NOW FOR OUR CYBER SECURITY SUMMIT

You’re invited to join us for our upcoming Cyber Security Event October 8 & 9 in Philadelphia, PA, featuring presentations on mobile application security, social media, advanced threats, corporate security, and more. Sign up now to reserve your spot and get more information!

Top Incidents

**Energy**

- Anti-fracking activists staged over 15 demonstrations at a series of sites around the UK, including alleged “aggravated trespass” into an office building used by shale gas explorer Cuadrilla in Blackpool. Police said they were investigating after “around 15 people forced their way into the office space” at about midday on Monday and stayed for three hours.

**Agribusiness**

- Russia said on Thursday it was investigating dozens of McDonald’s (MCD.N)
restaurants, in what many businessmen said was retaliation for Western sanctions over Ukraine they fear could spread to other symbols of Western capitalism.

**Insurance/Healthcare/Pharmaceutical**

- The well-known Community Health Systems, Inc. (CHSI) data breach that compromised 4.5 million patient data was a result of the OpenSSL Heartbleed.

**Financial Services**

- A major US shipping services provider announced a security breach on August 20, 2014 that affected 51 of its locations. Customers’ personal information, including credit and debit card data were compromised as part of the breach. The compromised locations experienced a malware intrusion but no fraud has been reported to date. The earliest evidence of the malware that affected the shipping stores dates back to Jan. 20, but the bulk of the locations were affected after March 26.

**Global Intelligence**

- Gamers woke up to an unpleasant surprise on Sunday morning when hackers brought down Sony’s PlayStation Network by way of a distributed denial-of-service (DDos) attack. The attack was followed up by a Twitter threat to an executive’s en route plane.

**Legal and Regulations**

- Earlier this month, Facebook announced a significant upcoming change to a section of its policies that will affect the way promotions may be administered on Facebook. Effective November 5, 2014, “like-gating” a page (i.e. requiring an individual to “like” a Facebook page) will no longer be allowed as a pre-requisite to entering a promotion or viewing content on a page or app. In short, Facebook has banned the practice of incentivizing consumers to like a Page.

**Energy**

- Nextgov reports that a dozen Nuclear Regulatory Commission (NRC) personnel were phished by email asking them to verify their user accounts by clicking a link and logging in. The link actually took victims to “a cloud-based Google spreadsheet.” According to an IG report hackers also attacked commission employees with targeted spear phishing emails that linked to malicious software.

- Thousands of people are set to form an 8km-long human chain across the German-Polish border August 23 in protest against a coal mining project. Climate activists from across Europe will join local protestors who could be forced from their homes if the mining plans go ahead. They plan to line up between Grabice, Poland and Kerkwitz, Germany, two of the villages that would be bulldozed to make way for coal pits. Some 6,000 people in the region are under threat of relocation.

- The location has finally been announced for the Earth First! Summer Gathering in the UK. Large-scale Earth First! Gatherings such as this typically culminate in a “graduation” event designed to disrupt the operation of a nearby business or facility of which the group disapproves. The announced location is South Downs Farm, Verrington, Charlton Musgrove, BA9 8JP.

- Anti-fracking activists are staging a protest on August 26 in Freeville, NY, to coincide with a NYSEG meeting over a proposed gas pipeline.

- The group Utah Tar Sands Resistance will be hosting events in the Book Cliffs on Sept. 12-15 & 19-21. The first event appears to focus on skills trainings, such as Tree Climbing. The second event appears designed to focus on networking and relationship building between members from various groups.
The Natural Resources Defense Council will be speaking about crude-by-rail risks at a forum in Martinez, CA on Sept. 8.

The Sept. 21 People’s Climate March that Bill McKibben is organizing in NYC is inspiring global clones. The People’s Climate March London will happen on the same day, and appears to be organizing around a similar model.

A group of Canadian anti-fracking activists in Moncton, NB is organizing a protest on October 11. The protest’s name, Global Frackdown, suggests that the group is expecting other anti-fracking protests throughout Canada and other countries on the same day.

Anti-fracking activists staged over 15 demonstrations at a series of sites around the UK, including alleged “aggravated trespass” into an office building used by shale gas explorer Cuadrilla in Blackpool. Police said they were investigating after “around 15 people forced their way into the office space” at about midday on Monday and stayed for three hours.

The World Wildlife Fund filed a complaint with the UK Advertising Standards Authority (ASA) against the world’s largest coal company, Peabody Energy, for ads it ran in the UK as part of a new PR campaign, “Advanced Energy for Life.” The ASA ruled that the ads, “Let’s brighten the many faces of global energy poverty,” were misleading and that Peabody should stop using the phrase “clean coal.” The company was told that future ads should neither state nor imply that their technologies are emissions-free unless they can prove that is true.

Microsoft said on Tuesday that it will end its involvement with the American Legislative Exchange Council, the conservative advocacy group, reportedly because of the group’s lobbying against renewable energy.

---

Agribusiness

- Russia said on Thursday it was investigating dozens of McDonald’s (MCD.N) restaurants, in what many businessmen said was retaliation for Western sanctions over Ukraine they fear could spread to other symbols of Western capitalism.

- The World Trade Organization has ruled in favor of Canada and Mexico in the six-year-old dispute over U.S. rules that require packages of beef, pork and poultry to carry labels saying where the meat was produced.

- China’s Agriculture Ministry decided not to renew permits that allowed development of three varieties of genetically engineered rice and corn. Some environmentalists say public unease over GE crops drove the decision. Other analysts say it was a matter of economics; China is nearly self-sufficient in rice so it does not need GE rice.

- An environmental blogger has raised $75,000 from donations over the Internet “to buy drones and other equipment to do investigative work tracking animal abuse and pollution problems on large livestock operations.”

- Skeptics of genetically engineered crops will speak during a National Research Council meeting on Sept and 16. A panel of experts was appointed by the council to look at the record of GE crops and future prospects. More than an hour was allotted for presentations from groups such as Food and Water Watch, the Center for Food Safety and Consumers Union.

- Russia’s legislative commission has approved a bill which increases fines for GMO labeling violations. Vague or unclear labeling of foods containing GMO’s can now be fined for up to $1,300 for individuals and up to $4,000 for business entities, and products can be confiscated.

- On August 20, 2014, themercury.com reported the state of Tasmania in Australia has
extended its GMO ban for at least another 5 years. Officials stated that "there is currently no imperative to change from having a moratorium."

- On August 20 it was officially announced that Initiative 105 requiring GMO labeling on foods in Colorado has been added to the ballot in November. The initiative was added after the submission of nearly 40,000 valid signatures more than the required 86,105.

- On August 21, 2014, Sustainable Pulse reports on a market report from Transparency Market Research which indicates that the global glyphosate market (valued at $5.46 billion USD in 2012) could reach a total value of $8.79 billion USD by 2019. According to the report, 45.2% of total glyphosate demand in 2012 was due to GM crops.

- On August 21, 2014, RT published a story about the recent decision by the Chinese Ministry of Agriculture not to approve the continuation of GM development. According to the story, on August 17, the permits for this GM development program were up for renewal and the ministry decided not to extend the program. The decision comes after recent discovery of GM strains of rice being sold on the open market which is illegal in China.

- California state bill AB 1789, also called the Big Corp Protection bill was passed this week. The bill which puts off decisions on changing or limiting pesticide use until 2020 has passed by a large majority with only one vote against. There is a 30 day window for the governor to sign the bill into law.

Insurance/Healthcare/Pharmaceutical

Insurance

- NYU Langone Medical Center had notified 8,400 patients of a stolen computer containing their protected health information.

- News of another massive hacker attack in the healthcare arena offers more proof that hackers are now hitting organizations in this sector because they're perceived as easier targets than those in other sectors, information security experts say.

- E.A. Conway Medical Center, part of the [Louisiana State University, LSU] University Health System, experienced a computer security breach on Tuesday that affected more than 6,000 patients, but no personal or sensitive information was compromised.

- Children's Mercy Hospital of Kansas City, Mo. recently alerted 4,076 employees' data may have been exposed in a breach involving its online scheduling.

- The well-known Community Health Systems, Inc. (CHSI) data breach that compromised 4.5 million patient data was a result of the OpenSSL Heartbleed.

- A Tucson health-care network accused of Medicare fraud has agreed to pay a $35 million settlement — the largest penalty of its kind in Arizona — and a whistle-blower who exposed the case will receive nearly $6 million of that sum.

- The Baton Rouge owner of three mental health centers was sentenced Monday (Aug. 18) in U.S. District Court in downtown Baton Rouge to pay $43.5 million in restitution and serve 8-and-a-half years in federal prison for a Medicare fraud scheme.

- After promising not to withhold government information over "speculative or abstract fears," the Obama administration has concluded it will not publicly disclose federal records that could shed light on the security of the government's health care website because doing so could "potentially" allow hackers to break in.

- When it comes to data breaches, hacking and loss or theft of unencrypted devices are far from healthcare security professionals’ only concerns. Employee snooping and insider misuse also prove to be among the biggest privacy threats in the healthcare sector.
Pharmaceutical

- The U.S. Drug Enforcement Administration is taking steps to restrict prescriptions of narcotic painkillers in a bid to curb abuse of pills taken by millions of Americans.

- The Justice Department on Friday filed additional charges against FedEx Corp, accusing it of conspiracy to launder money, in connection with its prescription-drug case against the package-delivery concern.

- AstraZeneca announced that it has received confirmation from the United States Department of Justice that it is closing its investigation into PLATO, a clinical trial with Brilinta (ticagrelor). The government is not planning any further action.

- No industry has been hit harder by hacking and data breaches than health care. Recent numbers show 90% of health care organizations have exposed their patients’ data -- or had it stolen -- in 2012 and 2013, according to privacy researchers at the Ponemon Institute. The medical industry faces more breaches than the military and banking sectors combined.

Financial

Activism

- Housing activists held an anti-eviction protest and press conference in San Francisco, CA on August 20th to bring awareness to unlawful and unjust eviction.

- Housing activists held a protest march against “home flipping and housing speculation” in San Francisco on Friday August 22nd.

- Housing activist groups are encouraging their supporters to protest at local U.S Department of Housing and Urban Development (HUD) offices nationwide on Tuesday, September 9th to demand better housing policies.

- Housing activists held an anti-eviction protest on August 18th at the county court house in Seattle, WA in support of a local family facing eviction.

- An activist group launched a petition against a leading U.S. bank that recently reached a $16.5 billion mortgage fraud settlement with the Justice Department, demanding that the bank meet directly with families affected by their mortgages.

- An anti-foreclosure activist group openly criticized the Justice Department for reaching a multibillion dollar mortgage fraud settlement with a leading U.S. bank instead of seeking justice for the bank’s customers, calling the deal a cover-up and a bail-out to those who intentionally broke the law.

- A housing activist launched a petition against a leading U.S. bank, demanding that the bank stop its deceptive practices regarding mortgage modification.

- An activist group will hold a demonstration outside the bankruptcy court in Detroit, MI on September 2nd against the state-enforced city bankruptcy trial that will begin on August 29.

- Housing activists held an anti-eviction blockade in Springfield, MA on August 22nd in support of a local homeowner facing eviction.

- A housing activist group held an anti-foreclosure protest on August 22nd in Lynn, MA in support of a local homeowner facing foreclosure.
Activists will stage a “Global Day of Action” in cities worldwide against a United Nations international financial institution on October 10th, protesting the institution's development policies that only favor big governments and corporations.

**Information Security Risk**

- A hacker group claimed to have downed the website of a regional Reserve Bank in St. Louis, MO under the flag of #OpFerguson.

- Operating under the flag of #OpArabia, a hacker group claimed to have downed the websites of national financial institutions in several Islamic countries in the Middle Eastern region.

- A UK payment processing company said data breaches have compromised nearly seven million UK credit and debit cards over the last three years, with breached businesses each paying out almost a million in forensic and remediation costs. According to the company, the three-year average per breached firm is now $1.475 million, which it calculated by summing a combination of forensic costs and fines generated by incidents it was aware of through industry reporting systems.

- A hacker broke into the state of Delaware’s treasury division website last week, posting an anti-Israel, pro-Palestinian message. The message stated in part, "Hacking sites will not stop unless Gaza is free." It is not known at what time the department’s normal webpage was taken over, but the entire website was restored within several hours.

- A yacht club in Chicago, IL said they experienced a computer security incident in which debit and credit cards of their high-profile members may have been compromised. The club’s official statement said their computer system failed on 15th June, 2014, and an IT forensics firm identified indicators that malware might have been positioned on one of the servers of the club between April 26th - May 22nd. The club’s official statement however mentioned that the server used for payments made through the website of the club is hosted by a third party and it is not involved in the incident and that bank account and credit card numbers were encrypted.

- A New Orleans restaurant said customers’ credit and debit card information could have been stolen by a hacker who breached the restaurant’s point of sale system between May 9th and July 18th. The business discovered that a hacker installed a previously unidentified malware called Backoff, which targets point of sale systems, on May 9th. Customers’ names, card numbers, expiration dates and CVV security code numbers were compromised. About 8,000 customers charged cards during the breach, a restaurant spokeswoman said.

- The website of a leading U.S. online vitamins retailer was attacked and payment cards and other customer information were compromised. The retailer learned of the incident on July 15th and closed the access point used by the attacker on July 17th. The attacker has not been caught, and an investigation is ongoing. Sources said anyone who made purchases on their website between April 22nd and July 17th may have had their personal information, including names, addresses, email addresses, phone numbers, passwords used to create accounts, credit and debit cards, expiration dates and CVV codes, compromised.

- The FBI’s Internet Crime Complaint Center (IC3) has issued an urgent warning about a major ransomware known as Reveton. The malware is described as drive-by malware because unlike many viruses—which activate when users open a file or attachment—this one can install itself when users simply click on a compromised website. Once infected, the victim’s computer immediately locks, and the monitor displays a screen stating there has been a violation of federal law. The bogus message goes on to say that the user’s Internet address was identified by the FBI or the Department of Justice’s Computer Crime and Intellectual Property Section as having been associated with child pornography sites or other illegal online activity. To unlock their machines, users are required to pay a fine using a prepaid money card service.
The malware is also used by hackers in conjunction with the Citadel malware, a software delivery platform that can disseminate various kinds of computer viruses. The Bureau suggests users not pay any money or provide any personal information and contact a computer professional to remove Reveton and Citadel from their computers. Victims also need to be aware that even if they are able to unfreeze their computer on their own, the malware may still operate in the background. Certain types of malware have been known to capture personal information such as user names, passwords, and credit card numbers through embedded keystroke logging programs.

- A hacker group announced that they launched a cyber-attack against a stock exchange in an Islamic nation in the Middle Eastern region. The hackers claimed the websites of the exchange were rendered inaccessible for nearly two hours. They also claimed the attack was launched in retaliation against the country's financial support for Israeli atrocities, and in protest of its violence toward prisoners in the country.

- Researchers said a leading U.S. bank’s customers are being targeted in a phishing campaign dubbed "Smash and Grab." It was launched on Tuesday, August 19th with a widely distributed e-mail that urged recipients to click on an included link to view a secure message from the bank. Users who click on the link are asked to enter credentials for accessing accounts with the bank. The researchers said even if users do not comply, the site will attempt to automatically install the Dyre banking Trojan on their PCs.

**Legal, Litigation, Regulatory Risk**

- The Securities and Exchange Commission announced charges against an accounting firm partner in Atlanta, GA for insider trading. Charges allege that the firm traded in the stock of a restaurant company based on confidential information learned from a client on the board of directors who came to them for tax advice in advance of a tender offer announcement. SEC investigators also identified and charged three other traders who traded illegally on tips from the accountant. The traders were discovered by comparing trading records from stock exchanges with names on the accountant's client list.

- The US Department of Justice has ordered a leading U.S. bank to pay $16.65bn to settle claims over selling risky mortgage securities prior to the 2008 financial crisis. As part of the settlement, the bank will pay $7bn as relief to affected homeowners. The bank is also required to pay a $5bn penalty under the Financial Institutions Reform, Recovery and Enforcement Act (FIRREA) and $4.63bn in compensatory remediation payments.

**Operational Risk**

- An article published last week stated that the Federal Reserve and Federal Deposit Insurance Corp.’s decision that the “living will” plans by 11 large banks submitted in 2013 are “not credible” may be an indication that regulators may be preparing to break up the mega-banks.

- Researchers said more than 400 organizations were recently targeted by a Bitcoin phishing campaign that intended to con users into disclosing their wallet passwords. 12,000 messages were recently sent in two waves to a handful of representatives across the higher education, financial services, high tech, media and manufacturing industry. The messages purport to come from the currency’s most popular transaction database, and warn the user that a hijacker was recently spotted trying to access their account. The alert gives details surrounding the alleged intrusion, including the date, IP address and location of the suspicious sign-in. Likely, in hopes of playing up to recent Chinese hacking stories, the location of the sign-in attempt is labeled as being from “Sichuan, GS, China.” Each message also has its own “CASE ID,” in hopes of tricking the user into thinking it’s legitimate. If users click through the “Reset Password” button, they’re led to a fake, yet authentic-looking Bitcoin transaction site. Not surprisingly, any information entered here, like a username or password, will get fired off to the attackers while users will get forwarded to a “generic login error message.” From there attackers would are free to make off with users’ Bitcoin.
Researchers said a new fraudster known as “MrMouse” on several top crime boards is selling counterfeit $20s, $50s and $100s, and claims that his currency will pass most of the tests that merchants use to tell bogus bills from the real thing. The researchers said judging from images of his bogus bills, the fake $100 is a copy of the Series 1996 version of the note — not the most recent $100 design released by the U.S. Treasury Department in October 2013. Customers who’ve purchased his goods say the $20 notes feel a bit waxy, but that the $50s and $100s are quite good fakes. MrMouse says his single-ply bills do not have magnetic ink, and so they won’t pass machines designed to look for the presence of this feature. However, this fraudster claims his $100 bill includes most of the other security features that store clerks and cashiers will look for to detect counterfeit money, including the watermark, the pen test, and the security strip. In addition, MrMouse says his notes include “microprinting,” tiny lettering that can only be seen under magnification (“USA 100” is repeated within the number 100 in the lower left corner, and “The United States of America” appears as a line in the left lapel of Franklin’s coat). This fraudster also claims his hundreds sport “color-shifting ink,” an advanced feature that gives the money an appearance of changing color when held at different angles.

Researchers discovered a new piece of malware that unleashes a trojan-horse called Krysanec, which is a type of Remote Access Trojan (RAT). Krysanec infects Android devices by masquerading as legitimate applications, and even displays dubious credentials of its creators, to trick Android smartphone users into downloading the app. After is is download the trojan opens backdoors for hackers to remotely gain access to user data. Once on a host device, Krysanec allows its creators to add extra functionality in the form of additional plug-in modules that can potentially upgrade the existing basic malware capabilities of Krysanec. The additional plug-ins, once executed and installed within the infected Android device, could allow the hackers to record audio via the device’s microphone, tap into the user’s text messages/contacts list, send text messages and even detect the user’s location with the help of the host Android device’s GPS functionality.

**Reputational Risk**

- A post published last week claimed that a US post-trade financial services company providing clearing and settlement services owns all the mortgages in the United States because all the securitized loans in the world will be held by the company.

**Global Intelligence**

**China**

- Hong Kong-based labor group SACOM (Students and Scholars Against Corporate Misbehaviour) posted a statement on their website demanding Apple to further improve labor conditions at supplier factories. The latest post is in response to Apple’s announcement on Aug 13 to ban the use of chemicals such as benzene and n-hexhane in final assembly facilities that produce iPhone and iPad products. SACOM expressed that Apple should expand the ban to all levels of its supply chain.

- China Mobile is planning service position cuts in Shandong, Fujian, Shanxi and other provinces. Laid off employees protested and demonstrated in front of local government buildings hoping officials would pressure the company to meet their demands.

- Taiwanese news outlet, Digitimes, reported that the Chinese government has announced a temporary stoppage on polysilicon imports through export processing zones (EPZs) beginning Sept 1, 2014, with the intention to block evasion of anti-dumping and anti-subsidization taxes.

- On 8/18/2014, a Chinese technology news outlet reports P2P network loan platform struggle in battling frequent hacker attacks. According to the article, the most common
attack experience by P2P network loan platform are distributed-denial-of-service attack.

- On 8/19/2014, a Chinese technology news outlet reports the trend on global Distributed Denial of Service attacks in the second quarter of 2014. According to the article, the number of botnet has increased and one of them called Brobot (itsoknoproblembro, a server-based botnet secretly lurking and ready for a strategic attack.

- On 8/20/2014, a Chinese technology news outlet provides updates on the large-scale DDoS attacks experienced by Hong Kong Civil Referendum's polling platform, PopVote in June, 2014 and causing the reference to be postponed.

- On 8/20/2014, a Chinese news outlet reports the Malaysia Airline Flight MH370 suspected to be hacked by Chinese hackers.

- On 8/21/2014, a Chinese news outlet reports the official website of a Chinese news outlet, Bjnews.com.cn suspects to have been attacked and hacked. According to the article, the domain name of the website were being modified twice on August 19th and 20th. The news outlet is still waiting for an explanation from the domain registration registrar, 35.com.

- On 8/21/2014, a Chinese news outlet reports a mutated strain of Linux Trojan are able to infect Windows XP, 7, and 8.1 platforms.


- On 8/22/2014, a Chinese news outlet reports a malicious trojan dubbed as "Locust" spread through more than 100 thousands user in approximately 10 hours and sent out large amount of unauthorized SMS messages.

- On 8/22/2014, a Chinese news outlet reports 360 Security's survey shows that there are 750 thousands routers out of 100 millions have experienced malicious DNS tampering. The survey shows that most 72% DNS tampering came from outside of China and 60.2% came from Korea.

**North America**

- Gamers woke up to an unpleasant surprise on Sunday morning when hackers brought down Sony's PlayStation Network by way of a distributed denial-of-service (DDoS) attack. The attack was followed up by a Twitter threat to an executive's en route plane.

- Researchers from the Tel Aviv University have demonstrated new and unexpected ways to retrieve decryption keys from computers. Their attacks have been leveraged against GnuPG. They measured fluctuations of electrical potential on the chassis of laptop computers by setting up a wire that connected to an amplifier and digitizer.

- Protests in Ferguson, Missouri have turned violent and looting has affected a number of businesses in the area, including Domino's Pizza, Papa John's, an auto parts store, grocery shop, technology store, and storage facility.

- Dollar General Corp. launched a takeover bid for Dollar Tree Inc. stores this week. In addition, the company is moving forward with plans to build its first stores in the state of Maine.

- Russia’s state food safety watchdog agency, Rospotrebnadzor, temporarily closed down four big McDonald's restaurants in Moscow on Wednesday allegedly due to “numerous sanitary violations,” the food safety agency said in a statement.

- American Clothing retailer Gap with enter India next year. The company plans to open 40 outlets across the country.

- New research studies show Americans started their back-to-school shopping earlier this year and the vast majority of consumers are using smartphones as part of the process.
Basic security issues in the networked system regulating traffic flow in Michigan allowed a team of researchers to take control of about 100 traffic lights. They managed to intercept the communication between traffic sensors and controllers that communicate wirelessly, gaining complete control of the stoplights regulating the flow of vehicles on the road.

A new report says Microsoft will give the world a first look at the new version of Windows on Sept. 30 or soon afterward at a press event to announce a developer build of the software.

More than 1,000 American businesses have been affected by the cyberattack that hit the in-store cash register systems at Target, Supervalu and most recently UPS Stores. The attacks are much more pervasive than previously reported, and hackers are pilfering the data of millions of payment cards from American consumers without companies knowing about it, according to a new Department of Homeland Security advisory released Friday afternoon.

Malaysia

- On 8/15/2014, a Malaysian news outlet reports police broke a syndicate selling medical certificates (MC).
- On 8/19/2014, MTUC reports Malaysia is opening all sectors to Bangladeshi workers and allowed them to work in all sectors.
- On 8/17/2014, a Malaysian news outlet reports Muslims religious leader calling to boycott in order to weaken Jewish economy.
- On 8/13/2014, a Malaysian news outlet reports the negative impact of McDonald restaurant's boycott due to its association to Israel has on the Muslim community in Malaysia.
- On 8/18/2014, a Malaysian news outlet reports the Malaysian Health Ministry’s Mental Health Promotion Advisory Council member Tan Sri Lee Lam Thye suggests that there should be policies at companies in private sectors to help its employees combat depression since many Malaysians spend at least 8 hours at work.

Legal and Regulations

- Earlier this month, Facebook announced a significant upcoming change to a section of its policies that will affect the way promotions may be administered on Facebook. Effective November 5, 2014, “like-gating” a page (i.e. requiring an individual to “like” a Facebook page) will no longer be allowed as a pre-requisite to entering a promotion or viewing content on a page or app. In short, Facebook has banned the practice of incentivizing consumers to like a Page.

- On August 12, 2014 in the case of Colin Cochran vs. Schwan’s Home Service, Inc. the California Court of Appeals ruled that “when employees must use their personal cell phones for work-related calls, Labor Code section 2802 requires the employer to reimburse them”? The Court determined “that reimbursement is always required. Otherwise, the employer would receive a windfall because it would be passing its operating expenses onto the employee.” Time will tell how BYOD tablets, laptops, and home computers are impacted by courts that follow the ruling in this case.

- On August 11th, the Consumer Financial Protection Bureau (“CFPB”) issued a consumer advisory warning consumers about the risks of virtual currencies such as Bitcoin. The CFPB advises consumers to be aware of potential issues with virtual currencies such as unclear costs, volatile exchange rates, the threat of hacking and scams, and that companies may not offer help or refunds for lost or stolen funds. The CFPB also announced that consumers who encounter a problem with a virtual currency
product or service can now submit a complaint with the Bureau.

- Payment Card Industry Security Standards Council (PCI-DSS Council) has released a useful guidance document for merchants accepting credit cards. The spate of data breaches is not the only reason that merchants should be paying attention to the guidance and reviewing it with care. The other reason is liability: when a merchant signs an agreement with a payment card processor (a “merchant agreement”), that merchant enters into a contract that includes an agreement to comply with the PCI-DSS rules, all of them. All businesses that handle payment card data (whether directly or through third parties) must become PCI DSS 3.0 compliant by December 31, 2014.

- Joining Yahoo, AOL issued a revised privacy policy last week (effective September 15) that inserted new language relating to so-called “do-not-track” signals. “There is no standard that governs what, if anything, websites should do when they receive these signals. AOL currently does not take action in response to these signals. If and when a standard for responding is established, we may revisit the policy on responding to these signals.”