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

In this white paper:
Social media has given activists and organizers free, powerful platforms to reach and connect to a wider audience of potential supporters, and maintain continuous communication with them once engaged. Moving beyond simple message dissemination, social media was also increasingly used to distribute propaganda, materials and increasingly structured training and tactics.

Top Incidents

**Energy**
- Blue Skies Montana, a group which recently had seven members arrested for obstructing a coal train in a protest, is using a recent oil train fire in Missoula to stir up fears of energy trains.

**Agribusiness**
Sustainable Pulse accuses the UK environment secretary of “breaching an agreement to make Scotland’s opposition to GM crops clear to European ministers”, failing to articulate Scotland’s different view on GMO from the UK at the EU Environment Council despite having previously promised to do so.

**Insurance/Healthcare**

- The FBI recently issued two alerts to the healthcare sector warning of increased risk of cyber-intrusions against systems and medical devices, especially as healthcare providers transition to electronic health records.

**Financial Services**

- Researchers warn that in the coming months, the network time protocol (NTP) amplification attacks will be replaced by new types of distributed reflected denial-of-service (DrDoS) threats. Researchers predict that in the next 12 to 18 months, many organizations will see attacks that exceed 800 Gbps.

**Worldwide Intelligence**

- Proposals have been made to update Canada’s federal privacy laws granting enforcement powers to Canada’s privacy commissioner and implementing to fine businesses up to USD 100,000 for not reporting data breaches. The proposed bill would also require businesses to track data breaches, communicate more clearly when gaining consent to collect personal data and facilitate the use and sharing of information amongst organizations. The bill now awaits second reading.

**Energy**

- Blue Skies Montana, a group which recently had seven members arrested for obstructing a coal train in a protest, is using a recent oil train fire in Missoula to stir up fears of energy trains.

- Calls for closing decades-old coal ash ponds at Duke Energy’s Asheville, NC plant picked up momentum this week with Gov. Pat McCrory urging that the utility be required to draw up a plan for making it happen and one the legislature’s top lawmakers promising to go a step further.

- Bill McKibben is promoting the “People’s Climate March” in NYC as “the biggest days ever in the climate fight.” The event is scheduled for Sept. 20-21.

- The 14 members of Hands Off Appalachia who were previously arrested for their role in an anti-coal action last November had a court appearance last week. HOA is using the occasion to solicit donations for their legal defense fund.

- 57 Greenpeace activists broke into a French nuclear facility, resulting in arrest.

- The “Big Mountain Spring Training Camp” is scheduled for May 16-23 on Big Mountain in Arizona.

- The organizers of the “Wild Roots Feral Futures” activist camp are seeking contributors in order to make a video to promote this year’s WRFF camp in Colorado.

- Scott Sagan, a senior fellow at Stanford’s Center for International Security and Cooperation, released a report claiming that the greatest dangers to nuclear facilities are sabotage and theft from insiders. “While there have been sabotage attempts in the United States and elsewhere against nuclear facilities conducted by insiders, the truth may be hard to decipher in an industry shrouded in security,” he said. “We usually lack
good and unclassified information about the details of such nuclear incidents,” Sagan said. The most recent known example occurred in 2012 – an apparent insider sabotage of a diesel generator at a nuclear facility in California. Arguably the most spectacular incident happened at South Africa’s Koeberg nuclear power plant (then under construction) in South Africa in 1982 when someone detonated explosives directly on a nuclear reactor.

- The US Fish and Wildlife Service has 18 active investigations of wind farms around the country, seven of which have been referred to the Department of Justice for prosecution. Since many of the easy to develop wind sites have already been developed new wind projects are increasingly at odds with bird, bat and environmental issues. The U.S. Fish and Wildlife Service (FWS), in concert with the Department of Justice (DOJ), is now actively pursuing cases of non-compliance with wildlife protection laws, especially those such as the Bald and Golden Eagle Protection Act and the Migratory Bird Treaty Act. Evidence of which was seen with the $1 million fine levied by the DOJ against a wind farm in Wyoming for eagle kills. Additional challenges may soon arise if the list of threatened and endangered species covered under the Endangered Species Act (ESA) is expanded to cover an additional 757 species.

- PG&E pleaded not guilty Monday to 12 criminal felony counts that allege the utility intentionally violated federal pipeline safety laws in connection with the 2010 natural gas explosion in San Bruno that killed 8 people, injured 66 and destroyed 38 homes. Were PG&E to be convicted on all 12 felony counts, the utility could face a fine of up to $6 million. But the penalties could exceed $6 million if the court finds that the company gained financially from its misconduct or if the victims' losses are taken into account, according to the U.S. attorney's office, which is prosecuting the case.

- UK MOP want to give energy companies the right to run shale gas pipelines under private land in an effort to “kick-start” the fracking industry. Ministers fear landowners and anti-fracking protesters would use existing law to block shale gas extraction in the UK, as it suggests prior permission is needed to run pipelines thousands of feet below private land. Prime Minister David Cameron has also indicated that the government could cut subsidies for land-based wind farms when it has "built enough to meet all our targets".

- Exxon Mobil shut one of Britain's main underground fuel pipelines, it said on Monday, after police found a stash of diesel they believe was siphoned off by thieves. Police arrested two men, aged 32 and 34, in connection with the theft. Media reported that more than 30,000 litres of diesel, worth 41,000 pounds ($70,000) at pump prices, was involved.

---

**Agribusiness**

- Babes Against Biotech is rallying support for Hawaii Rep. Jessica Wooley - currently the Hawaii House Ag Chair - whose confirmation as Director of the Office of Environmental Quality Control (OEQC) has allegedly been blocked by Sen. Nishihara. BAB urges readers to take action to support Rep. Wooley's confirmation to the position.

- An April 27 article by Sustainable Pulse accuses the UK environment secretary of “breaching an agreement to make Scotland's opposition to GM crops clear to European ministers”, failing to articulate Scotland's different view on GMO from the UK at the EU Environment Council despite having previously promised to do so.

- In an April 24 article Sustainable Pulse reports that a Friuli, Italy regional court has upheld a ban on MON810 in the region.
Insurance

- Federal officials are investigating the theft of personal information of about 8,830 former and current members of a Tufts Health Plan insurance plan, including names, birth dates, and Social Security numbers.

- Coordinated Health reported this week that a data breach involving a stolen laptop belonging to an employee may have affected up to 700 patients. The laptop contained protected health information (PHI) such as patient names, dates of birth, addresses, insurance information, appointment dates, and physician names, as well as Social Security numbers.

- Most healthcare IT security executives understand that no single solution will keep patient data secure and recognize that instead, a blend of the right technology, people and policy is the right approach. This multi-tiered approach leads to better security while allowing more efficient data management, sharing, and tracking.

- The Florida Supreme Court denied a petition to review a case involving the 2012 personal injury protection (PIP) reforms designed to help curb fraud and lower the cost of PIP insurance. Parts of these reforms were ruled unconstitutional before being upheld by the First District Court of Appeal; the case was then the Florida Supreme Court, which has now closed the case.

- The FBI recently issued two alerts to the healthcare sector warning of increased risk of cyber-intrusions against systems and medical devices, especially as healthcare providers transition to electronic health records.

- Dozens of old city records, some of which contained personal information for Quincy military veterans, such as Social Security numbers, bank account data, healthcare information and benefit claims, were strewn about a Quincy Center neighborhood Tuesday, the same day the city’s veterans service department disposed of thousands of old documents.

- Concentra Health Services (Concentra) has agreed to pay OCR $1,725,220 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and will adopt a corrective action plan to evidence their remediation of these findings.

- QCA Health Plan, Inc., of Arkansas, has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, agreeing to a $250,000 monetary settlement and to correct deficiencies in its HIPAA compliance program.

- Verizon released the findings of its “2014 Data Breach Investigations Report,” which reviewed and analyzed 10 years of data breach information and identified specific threat patterns, revealing a shift in focus by hackers from going after the dollar sign, such as the credit card or bank, to information, such as the healthcare industry.

- The Department of Health and Human Services is requiring consumers to change their passwords on the HealthCare.gov website as a precaution against the Heartbleed bug.

- Mark Swearingen, Shareholder at Hall, Render, Killian, Heath, & Lyman, discussed how providers will use the recently-released HIPAA Security Risk Analysis Tool and its long-term value to organizations of all shapes and sizes.

- Billing services provider Parallon Business Solutions recently notified the New
Hampshire Attorney General that a former employee had inappropriately accessed 40 New Hampshire residents' personal information. The 40 affected residents were patients at 13 different physicians' practices for which Parallon provided billing services.

- On Monday, HITRUST, in coordination with the U.S. Department of Health and Human Services (HHS), disclosed the results of the healthcare industry's first cyber-attack simulation exercise, CyberRX. It didn't release the full report, but held a press conference to discuss the findings and why industry collaboration is so important to healthcare-specific threat intelligence.

- A recent Office of Inspector General (OIG) report concentrated on how all 56 Medicaid agencies handle outsourcing administrative functions offshore, including whether they have HIPAA business associate agreements (BAAs) in place.

- The University of Pittsburgh Medical Center (UPMC) recently announced that as many as 27,000 of its 62,000 employees may have been affected by a recent data breach that exposed employee tax information, including Social Security numbers.

---

Financial

Activism

- Activists will hold a protest against the GMO industry at Philadelphia Stock Exchange on May 9th.

- Housing activists marched to a leading U.S. bank branch in Atlanta, Georgia on April 23rd and delivered a petition on behalf of a local construction company that's being foreclosed on by the bank.

- Activists will protest outside an undisclosed leading U.S. bank branch in Olympia, Washington on April 30th in observance of the ‘Earth Day to May Day.’

- Activists protested outside a leading U.S. bank branch in Winston-Salem, North Carolina on April 24th in solidarity of the ‘Earth Day to May Day’ action.

- Environmental activists held a vigil at the headquarters of a leading U.S. bank in Charlotte, North Carolina on April 22nd in observance of the ‘Earth Day to May Day.’

- Environmental activists on April 25th protested against a leading U.S. bank in Chicago, IL for funding the coal industry.

- Activists will launch a "march to and down Wall Street" action event on May 1st in New York City to denounce U.S. banks for destabilizing the labor market and economy.

- Environmental activists conducted a protest at the annual shareholders meeting of a leading U.S. bank in Tampa, FL on April 22nd, demanding that the bank end financing of the coal industry.

- Housing activists will hold a ‘May Day’ rally at the Hart Plaza in Detroit, MI on May 1st, followed by a march to downtown Detroit and Grand Circus Park to demand a moratorium on all bank and tax foreclosures, evictions and utility shutoffs.

- Activists protested at Balboa Park in San Diego, CA from April 26th to 27th to denounce U.S. banks’ investments in the fossil fuel industry.

- Activists protested outside a leading U.K. bank’s shareholders meeting in London on April 24th for their funding of mountaintop removal coal mining operations.
Activists will hold a protest against payday loan companies in London, UK, on May 1st.

**Information Security Risk**

- Security researchers have identified a dangerous variant of the ZeuS Banking Trojan that is signed by stolen Digital Certificates belonging to Microsoft Developers to avoid detection from Web browsers and anti-virus software. The P2P Zeus botnet is updating its bots/infected systems with versions that have the capability to drop a rootkit into infected systems and hide the Trojan to prevent the removal of malicious files and registry entries. The new variant also double checks for the earlier installed version (0x38) of ZeuS Trojan on the infected system and replaces it with updated binary files (0X3B version).

- A hactivist group on April 22nd claimed that they had successfully breached the systems of Singaporean financial firms.

- A European central bank is planning to employ ethical hacking and penetration testing in an effort to strengthen cyber security of banks and other financial institutions.

- A newly released study by a leading telecommunications & network security company found that hacking for espionage purposes is sharply increasing, with groups or national governments from Eastern Europe playing a growing role. According to the report, spying intrusions traced back to any country in 2013 were blamed on residents of China and other East Asian nations 49% of the time, but Eastern European countries, especially Russian-speaking nations, were the suspected launching site for 21% of breaches.

- IEX, an Alternative Trading System (ATS) that matches buyers and sellers of stocks, is attempting to combat predatory trading. The company behind IEX says the loophole exploited by high-frequency traders is in Reg NMS, which fails to specify the speed of the securities Information Processor (SIP). Therefore, IEX aims to combat predatory trading through the following measures: 350 microseconds of latency; No co-location; No special access to data; No kickbacks or rebates; Only four types of orders; No proprietary trading affiliates; Investor-owned only.

- A new study on botnets found that malicious botnets do most of their “dirty work” in the U.S. during dinner and after dinnertime. The study also found malicious bots account for nearly 24% of all web traffic, and “good” bot traffic actually dropped from 27.2% to 19.4%. The study says Pushdo remains the world’s largest botnet with 4 million bots and 4.2 million IP addresses sending spam and Trojans such as SpyEye and Zeus.

- The opening of the Johannesburg Stock Exchange (JSE) was delayed on the morning of April 23rd from 700 GMT to 800 GMT, after the JSE said that it had encountered a “technical issue” without expanding on the details.

- Security researchers report that real estate and title agencies are facing a new fraud scheme targeting consumers who are in the process of purchasing a home. In this scheme, the attackers intercept emails from title agencies providing wire transfer information for borrowers to transmit earnest money for an upcoming transaction. The scammers then substitute the title company’s bank account information with their own, and the unsuspecting would-be homeowner wires their down payment directly to the fraudsters.

- A hacker group on April 23rd claimed that they took down an American multinational financial services corporation with a DDoS attack. The attack was part of “Operation Payback” which was originally an Anonymous operation in retaliation for the 2010 shutdown of a popular file-sharing website that has transformed into campaigns targeting corporate interests or organizations in relation to the anti-Wall Street movement.
Researchers are warning of phishing emails related to the Heartbleed Bug. The phisher attempts to gather information by posing as a US military insurance service with a message about the Heartbleed bug. Users should note that the sender is using a very old mail client, Microsoft Outlook Express 6.00.2600.0000.

A new study on DDoS (Distributed Denial of Service) attack found more than 90% of respondents view DDoS attacks as a similar or bigger threat compared to the previous year, and that cybercriminals are using DDoS attacks to keep the targeted company’s IT staff distracted while they plant malware that’s designed to steal data. Close to half of the organizations that reported suffering a DDoS attack or a breach last year also had malware installed or activated on their systems. Furthermore, 55% of those targeted with DDoS attacks had funds, customer data or intellectual property stolen.

Numerous URLs belonging to many U.S. financial services firms were targeted by the “ZeuS GameOver with Necurs” malware through an unsolicited email from a toiletries company in a massive spam campaign.

Researchers warn that in the coming months, the network time protocol (NTP) amplification attacks will be replaced by new types of distributed reflected denial-of-service (DrDoS) threats. Researchers predict that in the next 12 to 18 months, many organizations will see attacks that exceed 800 Gbps.

Researchers say a cybercriminal operation that combines phone-based social engineering attacks with spear phishing and malware to steal money from organizations has resurfaced this year, finding victims in French-speaking countries in particular. Attackers send fake invoices to French-speaking accounting and finance department employees then follow up with phone calls impersonating managers and asking for those invoices to be processed. The rogue invoices are malware programs that allow attackers to gather sensitive information needed to transfer funds from the victim organizations to offshore accounts by abusing in-house accounting systems or by calling banks and impersonating company representatives. The most recent two attack campaigns, in February and April have used new Trojan program called Rokamal that can download and execute malicious files, steal information, open a backdoor on the infected computer, launch distributed denial-of-service attacks and mine cryptocurrency.

The Apache Software Foundation has released an advisory warning that a patch issued in March for a zero-day vulnerability in Apache Struts did not fully patch the bug in question.

Researchers warn that spammers are now replacing Latin characters with similar-looking symbols from other alphabets to evade spam filters. Non-Latin characters are inserted in place of similar-looking Latin characters both in the “Subject” field and in the body of the message. Using the UTF-8 coding system, characters from many types of writing systems can be combined within the same email.

**Legal, Litigation, Regulatory Risk**

The Securities and Exchange Commission (SEC) plans to review the cyber defenses of 50 Wall Street broker-dealers and investment advisers to determine whether they are prepared for potential cyber threats. The SEC Office of Compliance Inspections and Examinations (OCIE) will review each company’s tools and policies regarding governance, risk identification and assessment, network and data security controls, remote access, and third party cyber risks.

The SEC is weighing a requirement that brokers tell investors exactly where their stock trades go to be executed, a proposal that may address complaints that the decisions are sometimes made against the clients’ best interests. The SEC has said it’s reviewing every aspect of how stocks are traded, and regulators are trying to identify changes that might be implemented quickly.
• The SEC is reviewing whether certain alternative mutual funds that mimic riskier hedge-fund strategies are complying with leverage and liquidity rules, and plans to test around 25 of the funds over the next several months. The exams will shed light on how mutual funds are trying to generate yield and how much risk they are taking. They will help the Financial Stability Oversight Council determine whether it should designate some of the largest asset managers as systemically important, thus subjecting them to direct regulation by the Federal Reserve.

• The Massachusetts attorney general has launched an investigation into a data breach involving a subsidiary of a consumer credit rating company that resulted in the compromise of as many as 200 million records. Attorney generals in Illinois and Connecticut have also announced similar investigations.

• London Metropolitan Police reported nine members of a gang which carried out a sophisticated cyber-attack on the UK banking industry, stealing just over £1.25 million by remotely controlling bank accounts, have been sentenced to a total of 24 years and nine months imprisonment on Thursday, April 24th. The organized crime group also used bank and credit cards obtained from around one million intercepted or stolen letters to fraudulently purchase Rolex watches, designer jewelry and other high-value items, worth over £1 million.

• According to an April 7th report from Thomson Reuters, the United States Securities and Exchange Commission (“SEC”) has formed a group dedicated to the examination of private equity and hedge funds. The newly formed group will be co-headed by two veterans of the private equity and hedge fund sectors, Igor Rozenblit and Marc Wyatt. The rest of the group is initially expected to be comprised from existing staff across four SEC regional offices, with the possibility of expansion over the next twelve months.

• On April 10th, the FDIC issued a statement urging financial institutions to actively utilize available resources to identify and help mitigate potential cyber-related risks. In particular, the following organizations were mentioned: United States Computer Emergency Readiness Team U.S. Secret Service Electronic Crimes Task Force FBI InfraGard FDIC Press Release

**Operational Risk**

• Activist investors have written to a leading U.S. bank, urging it to disclose its climate risks and actively invest in solutions that will accelerate the transition to a low-carbon economy. Investors expressed their concerns about the consequences that fossil fuel investment will have on the planet and on their finances, given that up to 80% of known reserves will need to stay in the ground to avoid runaway global warming.

• Researchers monitoring the official Google Play market have identified Android apps that surreptitiously abuse end-user devices to carry out the computationally intensive process of mining Bitcoins. The malware, dubbed "BadLepricon," was stowed away inside five separate wallpaper apps that had from 100 to 500 downloads each.

• Researchers have identified a new Google Chrome extension that is targeting cryptocurrency users to steal Bitcoins and other crypto coins. The malicious Chrome browser extension dubbed ‘Cryptsy Dogecoin (DOGE) Live Ticker’ is available for free download on Chrome Web Store.

**Reputational Risk**

• An article accuses Attorney General Eric Holder of covering up mortgage fraud perpetrated by banks. The article claims Holder’s corrupt bargain, to let Wall Street walk, comes at the cost of permanent damage to the largest market in the world, the U.S. residential housing market.
· Hackers who recently raided the credit card payment system of a large U.S. retailer belong to a sophisticated Russian syndicate that has stolen more than 160 million credit-card numbers from retailers over seven years. The Russian group is well known to U.S. authorities, who have indicted several members and linked it to pillaging more than 100 companies.

· Russia is urging companies to delist their shares from overseas stock exchanges and trade in Moscow in an effort to safeguard them as international sanctions mount against the country after its takeover of Crimea. Further, the Russian government is creating “attractive” conditions for companies that decide to re-register on OAO Moscow Exchange, and will itself push on with plans to sell state-owned assets on the stock exchange.

· A U.S. District Court judge sided with the Federal Trade Commission’s (FTC) attempt to punish companies for poor security standards that lead to data breaches, as it refused to dismiss the agency’s lawsuit against a hotel and resort chain for getting hacked. The FTC claims the company’s promise to protect users’ data was “unfair and deceptive.”

· The Consumer Financial Protection Bureau recently ordered a leading U.S. investment bank to repay $727 million to consumers wronged by the bank’s deceptive marketing practices regarding credit card add-on products.

A U.S. university law school published a study that concludes minority residents in Minneapolis, MN are “much more likely than white people of similar incomes to be rejected for a mortgage, whether they’re buying a home or refinancing.” The study, using data from 2009 to 2012, focused more on general patterns than on particular bank activity. But it notes the “two largest banks in Minnesota would have made an additional 5,400 mortgage loans in racially diverse and mostly non-white Twin Cities neighborhoods during that period if they had distributed their loans proportionally to the distribution of homeowners with various incomes across the region.”

Global Intelligence

Canada

- Proposals have been made to update Canada’s federal privacy laws granting enforcement powers to Canada’s privacy commissioner and implementing to fine businesses up to USD 100,000 for not reporting data breaches. The proposed bill would also require businesses to track data breaches, communicate more clearly when gaining consent to collect personal data and facilitate the use and sharing of information amongst organizations. The bill now awaits second reading

China

- Chinese news outlets continued to report updates on the factory worker strike at Yue Yuen shoe manufacturing complex in Dongguan. On Sat. April 19th, the strike entered into its 5th day with 50,000 workers still involved, demanding the full amount in pensions and housing provident funds be paid to workers. Physical confrontations with police were reported as well as hundreds of arrests. Hong Kong labor rights group, Students and Scholars Against Corporate Misbehaviour (SACOM) posted an open letter on their website addressed to popular shoe brands urging the them to pay back benefits in full to all workers currently on strike at the Yue Yuen shoe factory. By April 23rd, many reportedly returned to work after the company made several concessions and local authorities increased pressure on workers to accept the deal. However,
some are still on strike, taking a stand against riot police stationed at factory entrances. In regards to labor union involvement, it appears that a lack of trust between employees and union representatives has complicated the union’s involvement in settling a negotiation.

Germany

- A shortage of qualified IT professionals might contribute to security risks in Germany according to the VDI, a professional association of civil engineers in Germany. There are roughly 2.5 available IT positions for college trained job-seeking professional overall, but 6.5 unfilled positions in IT security. Main reasons for the shortages are too few applicants and inappropriate or poor qualifications.

India

- Business Standard reported that Nokia officially communicated to its workers that the Chennai facility will become a contract manufacturing unit for Microsoft, which agreed to buy Nokia’s devices and services businesses globally, for Euro 5.44 billion.

Korea

- Global Post reported that the Federation of Korean Trade Unions, an umbrella labor union in South Korea, has cancelled an annual May Day rally as the entire nation remained immersed in grief and shock over a ferry disaster that killed at least 150 passengers on board.

North America

- WRAL TechWire reported that there may be an increase effort to get IBMers to carry union cards.

- QATAR Chronicle reported that Apple, Google, Adobe, and Intel have settled a lawsuit against involving an illegal no-poaching agreement which prevented them from hiring another's employees.

- Truth-Out reported that in 2013, the 10 biggest tech companies upped their spending on lobbying by 16% over the previous year. According the Truth-Out, the tech companies are casting a lot of their money toward causes that increase social and economic inequality, like pushing for cheaper labor and tax breaks for the richest of the rich. The article mentioned that with recent revelations about tech corporations getting paid to aid government spying as well as the wage-fixing scandal Intel and other tech companies’ reputation isn’t at a high point internationally.

- A new search engine allows individuals to search the Tor Market--commonly referred to as “DarkNet.” The search engine appears to imitate that of Google Search with the multicolored lettering and “I'm Feeling Lucky” search button. Users of the search engine must download the Tor browser bundle for access, which provides an extra level of anonymity. Once a user access the site, search results include marketplaces for items such as stolen credit cards, fake IDs and drugs. The beta version of the search engine is being tested as a release date has not been finalized.

- FTC On March 7, 2014, U.S. District Judge Esther Salas in New Jersey issued a much anticipated decision in FTC v. Wyndham Worldwide Corporation, et al., rejecting a direct challenge to the Federal Trade Commission’s (FTC) authority to police corporate cybersecurity practices. It would be wise for companies to review their cybersecurity practices in light of all relevant FTC rulings and statements to avoid issue with the the agency. While still subject to appellate review and not binding on other federal courts, Judge Salas’ decision paves the way for the FTC to seize the mantel as the top federal enforcement authority in the area of cybersecurity. A more complete discussion of the FTC v. Wyndham Worldwide Corporation, decision can be found on our blog at
On April 21, 2014, the Division of Corporate Finance of the Securities and Exchange Commission issued two new Compliance and Disclosure Interpretations (CDI) dealing with social media. The first CDI deals with how to affix required legends to tweets and other social media communications. The second CDI addresses retweeting or otherwise resending social media communications. The securities laws require certain communications by public companies to include legends. The mere length of these legends prohibited the use of social media like Twitter, because its 140 character limit would be exceeded. Now, the SEC has approved the use of Twitter or similar social media by permitting a hyperlink to the required legend instead of including the legend itself. There are conditions that must be met. The staff at the SEC has stated that they will be monitoring the use of social media in this context. They also indicated that if a social media platform allows for enough characters to include the legend, then the full legend must be included.

Following last June’s forum on mobile security, the Federal Trade Commission (“FTC”) again seeks to draw public attention to security issues in the mobile space. The FTC is soliciting comments from the public on a number of complex security issues discussed at the forum, including current privacy and data security risks in the mobile ecosystem, and the role mobile platform providers, telecommunications companies, third-party developers, and other industry members can play to mitigate mobile threats and to protect consumer privacy and security. The comments will expand the FTC record on these issues and will be considered in the drafting of an agency report.

The National Retail Federation announced this week that it will establish an Information Sharing and Analysis Centre for the retail industry in June to foster sharing of security information between the public and private sector. These measures are further to the Department of Justice and Federal Trade Commission’s recent announcement that companies would not breach antitrust laws by sharing information to mitigate or prevent cyber-attacks.

United Kingdom

- Supported by the pledge to provide “clarity to organisations on what good cyber security practice is”, the UK Government has launched its Cyber Essentials scheme setting out the steps to manage cyber risks. Funded by the National Cyber Security Programme, the scheme allows organisations to self-assess their cyber security protections and apply to be assessed and gain a ‘Cyber Essentials’ badge to demonstrate to their clients that they are ‘cyber safe’

Vietnam

- Intelligent Communication & More reported that Cisco Systems in Vietnam opened the Cisco Networking Academy Program in Hanoi and Ho Chi Minh City. The event was attended by high-ranking government officers, the Ambassador of the US as well as the attendance of enterprises and students of CNAP.