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
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Entertainment
- Defense
- Law Enforcement

2015 Security Trends Webinars
Join us in February for a three-part webinar series on mobile, information, and physical security trends.

Dates:
February 24, 25, & 26

Time:
10:00 AM PT | 1:00 PM ET

Top Incidents

Energy
- A coalition of concerned citizens from across the Northeast and Appalachia protested Dominion Resources’ analyst meeting held at the Waldorf Astoria. Dominion, one of the nation’s largest producers and transporters of energy, was promoting expansion projects of its subsidiary Dominion Midstream and its $3.8 billion Liquid Natural Gas (LNG) export terminal at Cove Point, MD.

Agribusiness
- The United States initiated consultations at the World Trade Organization over China’s
export subsidy system, announced U.S. Trade Representative Michael Froman. Consultations are the first step at WTO. If nations cannot reach agreement, the next step would be a request for a WTO panel to decide if trade rules are being violated. Agriculture is one of the seven areas identified by the United States as potentially getting unfair assistance.

**Insurance/Healthcare**

- Members of the National Association of Insurance Commissioners want a multi-state examination of Anthem, Inc. and its affiliates, following the discovery of a cybersecurity breach at the health insurance company.

**Financial Services**

- The largest British bank admitted failings by its Swiss subsidiary in response to media reports it helped wealthy customers dodge taxes and conceal millions of dollars of assets. The client list included many international celebrities, arms dealers, people linked to former dictators and traffickers in blood diamonds, and several individuals on the current U.S. sanctions list.

**Global Intelligence**

- An article on 17173.com reports that Electronic Soul, a Chinese online game developer, suffered a massive scale DDoS attack since the end of 2014 until recently. According to the article, the hacker group that is responsible for the attack has been arrested after a series of investigations collaborated on by Electronic Soul and the Chinese police force.

**Legal and Regulations**

- On February 10, the White House announced it will establish the Cyber Threat Intelligence Integration Center (CTIIC). In prepared remarks, Lisa Monaco, Assistant to the President for Homeland Security and Counterterrorism, revealed that the CTIIC will be responsible for integrating intelligence about cyber threats, providing analysis to policymakers and operators, and support the work of existing Federal government Cyber Centers, network defenders, and local law enforcement agencies. The set-up of the agency will operate under the auspices of the Director of National Intelligence.

**Pharmaceuticals**

- Financial institutions are getting smarter about fighting fraud. They are deploying multi-layered protection, and as a result, stealing credit card data or launching direct attacks on these institutions and customer bases is becoming increasingly complex. This is forcing hackers to look for alternative sources of financial gains. In 2015, there will likely be an increase in this type of attack outside of the financial sector. Look for attacks to expand into other verticals, including pharmaceutical companies, airlines, hotels, as well as into the lines of businesses within the enterprise.

**Retail**

- USA Today reported that the Mexican restaurant chain Chipotle had their Twitter feeds hacked early Sunday. After about 1 a.m. ET on Sunday, racially offensive and other insensitive tweets began emerging from the @ChipotleTweets account. The account’s profile picture of a pepper had been replaced with a swastika. The company later issued an apology tweet stating the account had been hijacked.

**Technology**

- Qualcomm Inc. might face an antitrust investigation in South Korea—not for the first time—underscoring its continuing legal issues after accepting a settlement with China earlier this week. South Korea’s Fair Trade Commission said Thursday it is considering an investigation into whether the big chip maker abused its dominant position in the market for smartphone technology. The agency in 2009 fined the company about $235 million after a three-year investigation, a ruling that is still under appeal.
Telecommunications

- A group of 43 municipal broadband providers are asking the FCC to exempt them from being included with large incumbent telcos and wireless operators as being common carriers under Title II of the Communications Act of 1934.

Defense

- The Defense Contract Management Agency, the U.S. federal government entity responsible for performing contract administration services for the Department of Defense, is responding to a suspected cybersecurity breach and has pulled a number of its servers offline while the investigation continues.

Law Enforcement

- A former U.S. Army sniper has pleaded guilty to conspiring to murder a DEA agent and an informant. Joseph Hunter, 49, and five others were arrested in September 2013 after they were recorded plotting to kill a DEA agent and informant in Liberia for $800,000. Hunter was snared in a sting operation in which he thought he was working for a Colombian drug cartel and faces between 10 years and life in prison when he is sentenced in May.

Energy

- An activist with the group, Stopping Extraction and Exports Destruction (SEED), climbed a 150 foot crane at a Dominion construction site that is part of the Cove Point liquefied natural gas export terminal project. She hung a banner reading, “Dominion get out. Don’t frack Maryland. No gas exports. Save Cove Point.”

- A coalition of concerned citizens from across the Northeast and Appalachia protested Dominion Resources’ analyst meeting held at the Waldorf Astoria. Dominion, one of the nation’s largest producers and transporters of energy, was promoting expansion projects of its subsidiary Dominion Midstream and its $3.8 billion Liquid Natural Gas (LNG) export terminal at Cove Point, MD.

- Australian uranium could end up in India’s nuclear weapons program thanks to concessions the Abbott government made in the deal between the two countries, two nuclear experts have warned. A former Australian diplomat and chairman of the International Atomic Energy Agency (IAEA), Ronald Walker, said the agreement to sell uranium to India “drastically changes longstanding policy” on safeguards and risked playing “fast and loose” with nuclear weapons. It differed substantially from Australia’s 23 other uranium export deals and “would do damage to the non-proliferation regime”, Walker told a hearing of the parliamentary joint standing committee on treaties this week.

- The French government has asked state-owned utility EDF to be transparent about its overseas operations to ensure that none were set up to avoid taxes, the finance ministry said on Sunday. In a letter addressed to the new head of EDF, Jean-Bernard Levy, Finance Minister Michel Sapin and Budget Minister Emmanuel Macron said they had asked the EDF board to supply such information at its next meeting. “While there may be technical, legal or commercial reasons for a company to have offices abroad, we cannot accept that such establishments are mainly guided by tax reasons,” said the letter, dated February 6 and seen by Reuters.

- Penn Energy reports that: New Mexico’s top environment officials and the U.S. Energy Department are wrangling over more than $54 million in fines levied in the wake of a radiological leak at the federal government’s underground nuclear waste repository. Now, state officials are threatening even more fines if the Energy Department doesn’t accept responsibility for numerous violations outlined in compliance orders issued by the state last year. The New Mexico Environment Department is working on a new
compliance order that could include fines of more than $100 million. Because negotiations with the federal government are ongoing, officials said the total penalties that could be assessed remains unclear. The Energy Department on Tuesday did not directly address the possibility of new fines, but it said the safe cleanup of its sites remains a top priority.

- Greenpeace New Zealand is launching a new members-only online platform for training and collaboration, called Greenwire.

- Texas fractivists are hosting a “lobby day,” busing people into the state capital on March 2.

- Sightline Institute, Earthjustice and Oil Change International are beginning to address what they believe is a series of “secret rulings” by the Bureau of Industry and Security to “erode” the oil export ban created by the 1975 Energy Policy and Conservation Act.

- Greenpeace New Zealand is using social media to promote its SecureDrop service for whistle blowers.

**Agribusiness**

- House and Senate sponsors announced a new drive in Congress to require labels on food made with genetically modified organisms.

- The United States initiated consultations at the World Trade Organization over China’s export subsidy system, announced U.S. Trade Representative Michael Froman. Consultations are the first step at WTO. If nations cannot reach agreement, the next step would be a request for a WTO panel to decide if trade rules are being violated. Agriculture is one of the seven areas identified by the United States as potentially getting unfair assistance.

- GMO-labeling legislation has been proposed in both the Florida House and Senate. The bill HB 351 was proposed by Representative Michelle Rehwinkel Vasilinda. In the Senate, the bill SB 416 has been proposed by Senator Jeremy Ring.

- Previously proposed GMO-labeling legislation has gained a total of 154 cosponsors out of 200 legislative districts. The bill will be given a new number and the go to consideration in a yet unassigned State House committee.

- The GMO-labeling bill SB 0734 has been introduced in the Illinois State Senate by Senator Dave Koehler along with five other co-sponsors. Sen. Koehler is the Chairman of the Senate Agriculture Committee and a supporter of GMO labeling.

- Food Sovereignty Ghana (FSG) has filed for an injunction on all GMO crops, especially GM rice and cowpeas, until government policies fully complies with existing GMO legislation. The suit is being brought against the Ghanaian National Biosafety Committee (NBC) and the Ghanaian Ministry of Food and Agriculture MoFA. FSG claims that Ghanaians are being wrongfully informed that attempts to import GM rice and beans are being conducted lawfully. FSG cites certain sections of Ghana’s Biosafety Act (2011) that are being violated.

- Traces of glyphosate have been found by researchers from Abraxis LLC and Boston University in a variety of products purchased in the Philadelphia metropolitan area. The researchers tested 69 honey samples, 26 pancake and corn syrup samples, 28 soy sauce samples, 11 soy milk samples, and 20 tofu samples. Most notably, 59% of honey samples contained glyphosate concentrations ranging from 17-163 ppb, with a mean of 64 ppb.

- In the beverage industry, niche categories are outperforming the rest of the market. Craft beer and wine are on the upswing as well as nutrient-rich and cold-pressed juices. Consumers are increasingly avoiding sugar substitutes in regular and soft
Food Production Daily reported that an Ontario, Canada court has levied a $70,000 fine against tomato processor Sun-Brite Foods, after a seasonal cannery worker was seriously injured while cleaning the plant.

Democrats Rep. Peter DeFazio and Sens. Barbara Boxer and Richard Blumenthal reintroduced The Genetically Engineered Food Right-to-Know Act. A federal bill that would mandate the accurate labeling of genetically-engineered ingredients in food or beverages sold in the US. The bill has been met with opposition from some corporations.

The Washington Times reported that in Wyoming, the Senate committee has endorsed a bill to deregulate the individual sale of raw milk, canned goods and other foods that are considered to be potentially dangerous. The Senate Agriculture, State and Public Lands and Water Resources Committee voted 3-2 on Thursday to advance House Bill 56, also known as the Wyoming Food Freedom Act. The measure goes to the Senate floor for more debate.

Insurance/Healthcare

- Insurance giant Anthem Inc. said Thursday that hackers had access to customer data going back to 2004 as investigations continue into the massive breach. The nation's second-largest health insurer disclosed the new time frame as it prepares to offer two years of free identity-theft protection to millions of affected consumers starting today.

- On February 5, the Article 29 Working Party (WP29) issued a letter to the EU Commission addressing a request to clarify the scope of health data in the context of well-being and lifestyle apps. In particular, the WP29 stated that, under the current Data Protection Directive (95/46/EC), further processing of mHealth personal data (even pseudonymised) for historical, statistical, and scientific research purposes should only be permitted with the explicit consent of data subjects, with exceptions laid down in national law.

- Health professionals have been caught snooping into former mayor Rob Ford’s medical records in four separate privacy breaches in at least three Toronto hospitals. Former mayor Rob Ford’s medical records being inappropriately accessed by hospital staff highlights the importance of upgrading Ontario’s health privacy laws.

- The hack attack against Anthem Inc., which the health insurer says started with a spear-phishing campaign targeting five of its employees, is a warning sign of the kinds of sophisticated schemes that will be common in the year ahead.

- In the wake of the cyber-attack against health insurer Anthem Inc., New York’s Department of Financial Services has announced plans to conduct “regular, targeted assessments of cybersecurity preparedness” for all insurers doing business in the state.

- Members of the National Association of Insurance Commissioners want a multi-state examination of Anthem, Inc. and its affiliates, following the discovery of a cybersecurity breach at the health insurance company.

Financial
Financial Services

Activism

- Activists in Greece held a protest against European Union austerity measures and the government’s attempts at curtailing public spending at Syntagma Square in Athens on February 11. Solidarity protests occurred internationally, including an action in front of the European Central Bank in Frankfurt, Germany.

- India's banking workforce will conduct an indefinite strike throughout India starting March 16 over wage disputes.

- A labor group representing public workers in the State of California held a rally on February 11 in San Francisco, demanding that San Francisco Employee Retirement System (SFERS) management stop investing 10% of the group’s pension funds into "speculative" hedge funds.

- Occupy Wall Street offshoot Strike Debt Bay Area hosted a planning meeting on February 14 in Oakland, CA to plan “awareness and resistance” actions focused on “unjust debt.”

- Activists will conduct an anti-gentrification protest on February 17 in Seattle, WA.

- Activists organized at a church in Providence, Rhode Island on February 12 to protest the CEO of a leading U.S. bank who provided the church’s service lecture on corporate social responsibility.

- An Australian labor union will hold a rally in Carlton South, Australia on March 4 to protest the Liberal Government's planned "Productivity Commission."

- Activists conducted anti-fossil fuels ‘Global Divestment Day’ actions in London, UK on February 13 and 14. Participants highlighted the devastating consequences of such fossil fuel investments, and demand that London goes fossil-free.

Information Security Risk

- Cybercriminals in Brazil are focusing on a new method of stealing Boletos, a nationwide payment method, by poisoning the domain name system (DNS) entry used by a bank’s website so that the IP address to the legitimate location points to a site controlled by the cybercriminals.

- A Chinese cybercriminal group known as the Yanbian Gang is using mobile malware to steal money from South Korean bank customers. The cyber gang has been transferring up to US$1,600 worth of local currency from victims’ accounts every day since 2013. The group is attributed with the creation of almost a thousand fake versions of Google Play App, which comes pre-installed on Android devices. The distribution of the malicious applications is done through links in mobile text messages (smishing - SMS phishing) or by getting them downloaded by other malware planted on the victims’ devices.

- Research highlighted that 25% of workers in the UK from 2013 to 2014 lost data due to the malfunction or corruption of technology. This is up from 19% just over two years ago. The report also uncovered that 33% of UK employees used personal devices or cloud services to store work-related data in the last 12 months. Unfortunately, recovery rates of lost work-related data among these devices are low. About 19% of users successfully recovered lost data from home desktops, but just 8% were able to do so from personal mobile devices, and 17% from laptops and tablets.

- An Omaha, NE-based commodities trading company founded 120 years ago lost $17.2 million in an international email swindle, according to federal court documents. An executive with the 800-employee company wired the money in installments last summer to a bank in China after receiving emails ordering him to do so. The gambit involved emails sent to one of the company executives that was purported to be from its Chief Executive Officer and the company’s outside auditing firm. The emails
The Defense Contract Management Agency, the U.S. federal government entity responsible for performing contract administration services for the Department of Defense may have suffered a cybersecurity breach and pulled a number of its servers offline while the investigation continues. A notice posted to the DCMA’s home page communicates little about the investigation, other than to note that “corrective action is in progress,” and that “work is being done to restore service as quickly as possible.”

A hacker group claimed to have taken down the official Chinese website of a leading American credit card service provider.

Researchers claimed that the website of a leading American financial news organization was infected by Chinese hackers with spying software that targeted specific visitors, including those at U.S. financial services and defense firms. The hackers infected the website in November 2014 with software that automatically attacked visitors by exploiting security flaws in Microsoft’s Internet Explorer browser and Adobe Systems’ Flash software.

The Twitter account of a leading American weekly news magazine was hacked last week by a group calling themselves the “Cyber Caliphate.” The group claimed to be affiliated with the Islamic State (ISIS) and have previously hacked @Centcom, the Twitter account of the United States Central Command, as well as the official Twitter account of Taylor Swift.

Legal, Litigation, Regulatory Risk

The Securities and Exchange Commission (SEC) sued a Cayman Islands-based bank and four other companies, claiming that they took more than US$75 million from unregistered sales of “virtually worthless” penny stocks. The U.S. regulator claimed these businesses filed bogus registration statements with the SEC, purporting to register securities to public shareholders, though there were no such sales and the securities stayed in the control of the issuers and their affiliates. In the sham offerings, the issuers pretended to sell securities to shareholders in such places as Serbia, Mexico, Ireland, Norway, Panama and Jamaica. The restricted securities were then “passed off” as free-trading stocks in the United States and sold to the public.

A former bank president was charged last week for his role in a bank fraud scheme in which he is alleged to have hidden under performing and at-risk loans from the bank and the Federal Deposit Insurance Corporation (FDIC), among others. The former banker was allegedly engaged in a long running scheme to mislead the bank and its loan committee about loans the bank made to local individuals and businesses. As part of the scheme, the former president allegedly hid past due loans from the FDIC and the bank loan committee, which resulted in the bank continuing to approve and renew delinquent loans and loans for which the collateral was lacking. Several of the borrowers eventually defaulted on the loans, resulting in millions of dollars in losses to the bank and others. He also allegedly hid his personal and business interests in at least two of the transactions over which he exercised approval authority.

The Federal Reserve said February 12 that results of its latest bank stress tests will be released on March 5 at 4:30 p.m. EST.

President Obama signed an Executive Order on February 13 aimed at encouraging companies to share more information about cybersecurity threats with the government and each other. The order sets the stage for new private-sector led “information sharing and analysis organizations” (ISAOs) - hubs where companies share cyber threat data with each other and with the Department of Homeland Security.

Operational Risk

Hong Kong’s central bank warned against investing in virtual currencies, amid local media reports that a Bitcoin exchange may have run off with $387 million in client
funds in what could be the biggest Bitcoin scandal after last year’s bankruptcy at a Tokyo-based exchange. The Hong Kong Monetary Authority said in a statement late Monday, February 9 that the case may involve fraud and urged the public to exercise extra caution when considering making transactions or investments with Bitcoin.

- An article reported that clashes over strategy within a leading U.S. bank’s compliance operations have led to the departure of a series of managers in the past year. The new strategy has created friction with some current and former bank managers who have more of a traditional law enforcement background and are used to doing their own in-depth probes of transactions. They claim the bank is emphasizing quantity over quality in its investigations.

Global Intelligence

Brazil

- Grappling with tumbling auto sales and weak economic growth, Brazil wants to derail a pact that would allow unlimited imports of cars from Mexico, sources familiar with the situation say, in a move that could stoke trade tensions between Latin America’s largest economies. Brazil this week invited a Mexican government delegation to a meeting in Brasilia between February 20 and 25 for talks to revamp the treaty.

- “The allegations against Petrobras are so egregious we have no choice but to take action on behalf of Ohio’s public employees and retirees,” DeWine told reporters in Columbus on February 9. Ohio is the latest plaintiff to pile on in a widening class action case against Latin America’s premier state-owned oil major, where evidence of pillage grows by the day.

- The possibility of leaving the largest metropolis in South America - Greater São Paulo is home to 20 million people - without water five days a week seems to be the worst-case scenario envisioned by Sabesp. But most analysts fear that unless there is a “downpour of Biblical proportions”, a co-ordinated system of water supply restrictions will have to be implemented in the coming weeks.

- The key money handler of the Petrobrás graft case testified that 11 federal contracts since 2004 worth 32.6 billion real had a standard one percent payment to the Progressive Party, allied with the President’s Workers Party. Evidence shows the party received 326 million reals in payments.

China

- An article on Nextmag.com reports that Macau’s governmental website suffered hacker attacks and the introduction video of a railway project was swapped to a pornographic video clip.

- A forum posting on It-home.org reports a security vulnerability on Android that could be exploited to gain access on the device’s camera. The user also posted source code that is able to exploit the vulnerability and send the images to specific servers.

- An article on Caikeji.com reports a design flaw on WhatsApp, where the functionality to let others know if the user is online could be exploited by software and allow hackers to access the user’s profile picture, change the user’s privacy setting, as well as status information.

- An article on 7down.net reports that malicious applications have been exploiting the trend of a popular festive social media game called “Red Packet” populated by Alippay and QQ. These malicious applications exploit the game and are able to intercept the victims’ text messages in order to collect personal, banking, and credit card information. “Red Packet” is a game which coincides with the upcoming Lunar New Year where players could win prizes and credit.
A Chinese news outlet reported on a P2P loan service provider that specializes in investment in the jewelry industry, Zhubao dai.com, experienced a DDoS attack on the night of February 11 which rendered the website out of service.

An article on Xinhua.net reports a malware spreading via QQ Group that not only could infect PCs, but also Android and iOS devices. This malware tricks victims to pornographic websites to download and install a malicious program disguised as a video player that promotes multiple malicious applications that attack Windows, Android and iOS devices.

An article on Sina.com.cn reports that 8Europe.com, an e-commerce site between Germany/Europe and China suffered massive-scale DDoS attacks on January 28, 2015. According to the article, the site has returned to normal and users have been able to login since February 2, but the attacks have not stopped.

A blog posting on Hkphp.cn reports that a new variant of the online banking malware, DYRE, is not spreading via Microsoft Outlook. The recent version of DYRE is able to bypass anti-virus software and infect victims by sending spam email to victims that contain an attachment of the UPATRE downloader (TROJ_UPATRE.SMBG).

An article on 17173.com reports that Electronic Soul, a Chinese online game developer, suffered a massive scale DDoS attack since the end of 2014 until recently. According to the article, the hacker group that is responsible for the attack has been arrested after a series of investigations collaborated on by Electronic Soul and the Chinese police force.

Yahoo!News reported that the Deputy Director of the Family Planning Commission of Shanxi province, offered recommendation to change China's policy and system to allow parents in China to have two children. The Deputy Director indicated that under his proposed policy change, the parents in China "must have two children." In an effort to rein in population growth, China in the late 1970s introduced its controversial family planning policies, which limit most couples to only one child. The regulations have led to sometimes brutal crackdowns on families with more than one child, including forced abortions and sterilization as well as the levying of hefty fines. The ruling Communist Party moved to relax the rules in late 2013 to allow couples to have two offspring so long as at least one of the parents is an only child. Yet far fewer couples have applied to have a second child than expected.

North America

Yahoo! News reported that Yahoo laid off a round of workers this week, mostly cutting back its news and entertainment division in Canada. Yahoo did not disclose if it laid off employees in California, but it was fewer than the 50 that would have triggered a required notification to the workers in advance. Neither the state nor the local workforce investment board nearest Yahoo's Sunnyvale headquarters received any notice from the company.

Business Insider reported that Halliburton announced that it will lay off between 5,000 and 6,500 employees. The drop in oil and gas prices has caused Halliburton's output to decline.

Business Management Daily reported that during an all-staff meeting at an Arizona warehouse, a worker voiced concerns about a safety issue. After the meeting, supervisors took the man aside and told him he was disrespectful and spoke too loudly during the meeting. The employee responded that he had to speak loudly to be heard. He was given a verbal reprimand. The employee complained to the National Labor Relations Board (NLRB), which eventually found that Amazon's rule requiring employees to always act "in the best interest of Amazon" to be overly broad. The NLRB said the rule could have a chilling effect on employees discussing working conditions.

Times Union reported that the Boston Consulting Group predicts that investment in industrial robots will grow 10% a year in the world's 25-biggest export nations through 2025, up from 2% to 3% a year now. The Boston Consulting Group predicts robots will
cut labor costs by 33% in South Korea, 25% in Japan, 24% in Canada and 22% in the United States and Taiwan. Only 10% of jobs that can be automated have already been taken by robots.

- The Communications Workers of America issued a statement claiming that CWA and more than 50 other labor, public interest, faith, community, and civil rights organizations have formed the Grand Alliance to Save Our Public Postal Service. According to the post, USPS management has been trying to push to outsource the work—to Staples stores, particularly—and shut down post offices. According to the post, the coalition will fight back against the forces that want to privatize the public postal service.

**Vietnam**

- Vietnam.Net reported that Bach Khoa Anti-virus Center (BKAV) last week reported that 1,600 computers in Vietnam had been infected with CTBLocker, a dangerous ransomware infection that decrypts files on computers and displays a so-called ransom warning. CTBLocker, a variant of CryptoLocker ransomware, has spread very rapidly in recent days. A BKAV report released on January 23 showed that 1,300 computers were infected with the ransomware, while an updated report on February 5 said the number increased by 300. According to BKAV, the number of CTBLocker’s victims could be much higher, because many of them had not reported the infection.

**Legal and Regulations**

- While patents have the Patent Cooperation Treaty and trademarks have the Madrid System for applying for IP rights internationally, there has generally been less international cooperation in the field of the protection of designs. The Hague System for protecting international designs has been in existence in one form or another since the 1930s, but its relatively poor coverage has to date made it much less attractive – and so less frequently used – than its cousins in other fields. At present, any company or person with nationality or residence in a Hague country – which includes all of the European Union – can file a Hague design application, but the coverage outside of the EU is patchy at best. This is likely to change shortly, as the United States and Japan deposit their instruments of accession to the Hague Agreement February 13, 2015. The Hague Agreement should therefore enter into force in those countries as of May 13, 2015.

- On February 10, the White House announced it will establish the Cyber Threat Intelligence Integration Center (CTIIC). In prepared remarks, Lisa Monaco, Assistant to the President for Homeland Security and Counterterrorism, revealed that the CTIIC will be responsible for integrating intelligence about cyber threats, providing analysis to policymakers and operators, and support the work of existing Federal government Cyber Centers, network defenders, and local law enforcement agencies. The set-up of the agency will operate under the auspices of the Director of National Intelligence.

- On January 21, Federal Trade Commission (“FTC”) Bureau of Consumer Protection Director Jessica Rich outlined in a speech before advertising industry professionals how businesses using targeted advertising may avoid legal trouble with the FTC and other authorities. As online tracking technologies evolve, companies should consider Rich’s recommendations as best practices in order to mitigate the risk of FTC scrutiny, especially when crafting data privacy policies and notices to consumers and also when contracting with third-party service providers.

- Many of the nation’s leading cyber, data and privacy experts convened Friday at a White House Summit at Stanford University to discuss ways to improve our nation’s cybersecurity. During the summit, President Obama signed an executive order to promote private sector cybersecurity information sharing. The summit focused on the following key areas:
Public-Private Partnerships
Protecting Consumers
Making good security part of good business
Securing payment systems

On February 3, the Financial Industry Regulatory Authority (“FINRA”) issued two publications concerning cybersecurity risks at financial firms. The *Report on Cybersecurity Practices* presents the results of FINRA’s 2014 targeted examination of cybersecurity issues at financial institutions and identifies risk management principles and practices to help firms reduce their exposure to cybersecurity threats. In conjunction with the report, FINRA also released *Cybersecurity and Your Brokerage Firm*, an investor alert designed to “encourage investors to understand a firm’s cybersecurity policies and take personal precautions to safeguard their brokerage accounts and personal financial information.” FINRA issued these publications on the same day as the U.S. Securities and Exchange Commission released its *Cybersecurity Examination Sweep Summary*, which presents observations from the SEC’s Office of Compliance Inspections and Examinations’ cybersecurity examinations of various financial institutions. For additional coverage of the SEC’s report, please see King & Spalding’s Client Alert, *SEC Releases Results of Financial Industry Examination Sweep Regarding Cybersecurity*.

Pharmaceuticals

- Security experts are warning healthcare and insurance companies that 2015 will be the “Year of the Healthcare Hack,” as cybercriminals are increasingly attracted to troves of personal information held by U.S. insurers and hospitals that command high prices on the underground market.

- In another sign Sanofi is struggling to remake itself, the drug maker is shrinking its oncology business and folding it into the Genzyme unit as part of a wider R&D reorganization. The move, which involves eliminating 100 R&D jobs in Massachusetts, comes as the drug maker struggles to bolster its key diabetes business and hire a new chief executive officer.

- Actavis plans to cut another 40 jobs in April, after eliminating 200 positions last month and another 48 in October.

- AstraZeneca has agreed to pay the federal government $7.9 million to settle allegations the drug maker paid kickbacks to a large pharmacy benefits manager to ensure that its blockbuster Nexium heartburn medication was given the best status on formularies, which are the list of drugs that received preferred coverage.

- A year after taking a seat on Ariad Pharmaceuticals’ board, activist investor Alex Denner is looking to oust CEO Harvey Berger, CNBC reports. Denner’s Sarissa Capital, the company’s largest shareholder, has stayed quiet over the past year, but with Berger up for reelection this year, the firm wants to see a change, according to CNBC. And Ariad can avoid a public proxy fight if it’s willing to strike a deal with Denner’s group, CNBC’s sources said, possibly spelling the end for Berger, the company’s founder known for his bullishness and public bluster. Denner first got involved in Ariad in 2013 when escalating safety concerns over the drug Iclusig sent it on a value-raiding downswing.

- Financial institutions are getting smarter about fighting fraud. They are deploying multi-layered protection, and as a result, stealing credit card data or launching direct attacks on these institutions and customer bases is becoming increasingly complex. This is forcing hackers to look for alternative sources of financial gains. In 2015, there will likely be an increase in this type of attack outside of the financial sector. Look for attacks to expand into other verticals, including pharmaceutical companies, airlines, hotels, as well as into the lines of businesses within the enterprise.