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

Cyber Safety Awareness Training

Protect your Organization with Computer-Based Training

Are your employees the weak link in your security program? We want to help you educate your employees to keep them – and your organization – more secure.

Our computer-based cyber security training can help your employees learn how to protect your organization from the latest threats and reduce the high costs associated with incident remediation.

Click Here To Learn More

Top Incidents

Energy

- U.S. Senator Charles Schumer is pushing federal regulators to expedite their rulemaking on DOT-111 train cars still being used to transport highly volatile crude oil across New York State. The train cars could potentially put local communities in danger given they are prone to rupture and explode during derailments.

Agribusiness

- While urban America has nearly universal access to wired broadband, the rate in rural America is 78 percent, according to industry data. USDA’s 2012 Census of Agriculture says 70 percent of farms have Internet access but a third of them use dial-up, satellite or mobile connections “that may not be adequate when it comes to accessing and delivering the large quantities of data that are associated with some precision.
agriculture processes,” write Brian Whitace, Tyler Mark and Terry Griffin in Choices, the journal of agricultural economics. “The availability of broadband for farm offices and land in production has serious implications for the future of agriculture.”

**Insurance/Healthcare**

- Beginning in early 2015, the Office for Civil Rights’ plans to audit 200 covered entities, including healthcare providers and group health plans, to measure their compliance with the HIPAA privacy, security, and breach notification rules requirements. These audits of covered entities will be followed by up to 400 audits of business associates to measure their compliance with the security rule and how they intend to approach their obligations under the privacy and breach notification rules.

**Financial Services**

- A leading U.S. investment firm fired one of its financial advisers after it accused him of stealing account data on about 350,000 clients and posting some of that information for sale online, in potentially the largest data theft at a wealth-management firm.

**Global Intelligence**

- A Chinese security news outlet reports a security vulnerability on wireless routers that use admin/admin as username/password could be exploited by embedding a malicious webpage. Once users visit the malicious page, the router’s DNS IP address will be modified, and personal information like banking information could be obtained.

**Legal and Regulations**

- The International Standards Organization’s new cloud standard, ISO 27018, strives to ensure that public cloud service providers (such as Amazon, Google, and Rackspace) “offer suitable information security controls to protect the privacy of their customers’ clients” by securing the personally identifiable information (PII) entrusted to them. The new standard, adopted by ISO and the International Electrotechnical Commission in August, is voluntary. It is expected to be followed by ISO 27017, which will cover non-privacy information security aspects of cloud computing. According to the ISO, the new standard is intended as “a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system ….” Broadly, ISO 27018 addresses the questions of confidentiality and security of the customer’s personal information and the prevention of its unauthorized use.

**Pharmaceuticals**

- China will allow online sales of prescription drugs as early as this month, a policy that will open up an over 1 trillion yuan ($161 billion) market to online pharmacy operators like Alibaba Group Holding Ltd and Wal-Mart Stores Inc.

**Retail**

- According to findings from IBM, the number of cyber attacks against US retailers has declined 50%, however, the number of records stolen from them remains at near record highs. Contrary to expectations, cyber attackers scaled back on Black Friday and Cyber Monday 2014 hacking efforts.

**Technology**

- New research out from the GlobalWebIndex indicates that in a survey of 170,000 adult Internet users across 32 markets, only 9% report having a smartwatch, and 7% said they owned smart wristbands. In contrast, among online adults, 80% now own a smartphone.

**Telecommunications**

- A group of Democratic leaders have incited a new political debate over what direction net neutrality should take by reintroducing a bill that would put a ban on paid prioritization agreements between content providers like Netflix and ISPs like AT&T and Verizon.
**Entertainment**

- The FBI revealed more details related to the Sony investigation. It claims that messages sent by the attackers were detected and showed that they were IP addresses only used by North Korea. Some experts still believe Sony employees may have been the culprits, whether it was an isolated incident or a joint effort with North Korea.

**Defense**

- Hackers claiming to be aligned with Islamic State militants took control of the U.S. Central Command’s Twitter and YouTube accounts Monday, posting phone numbers of top military officers and what they said were classified documents.

**Law Enforcement**

- French law enforcement officers have been told to erase their social media presence and to carry their weapons at all times because terror sleeper cells have been activated over the last 24 hours in the country, according to a French police source. Amedy Coulibaly, a suspect killed Friday during a deadly kosher market hostage siege, had made several phone calls about targeting police officers in France, according to the source. It was also reported in a French-language magazine that brothers Cherif and Said Kouachi had been under watch by the French, but despite red flags, authorities there lost interest in them.

---

**Energy**

- On July 3, 2014, DHS, responding to a Freedom of Information Act (FOIA) request on Operation Aurora, a malware attack on Google, instead released more than 800 pages of documents related to the Aurora Project, a 2007 research effort led by Idaho National Laboratory to show the cyber vulnerabilities of U.S. power and water systems, including electrical generators and water pumps. The research project found that once these infrastructure systems are infiltrated, a cyberattack can remotely control key circuit breakers, thereby throwing a machine’s rotating parts out of synchronization and causing parts of the system to break down. Responding to concerns that DHS had released the wrong information, a DHS spokesman told Defense One, “As part of a recent Freedom of Information Act (FOIA) request related to Operation Aurora, the Department of Homeland Security (DHS) National Programs and Protection Directorate provided several previously released documents to the requester. It appears that those documents may not have been specifically what the requester was seeking; however, the documents were thoroughly reviewed for sensitive or classified information prior to their release to ensure that critical infrastructure security would not be compromised.”

- A recent conference call for environmental groups including, "Rain Forest Action Network" and "Change the Course" discussed organizing civil disobedience actions across the country to resist all forms of fossil fuel related infrastructure. These actions appear to stem from the upcoming vote on the Keystone XL pipeline.

- The AARP is organizing public opposition to a proposed power purchase agreement in Ohio, that environmental and consumer advocates are painting as a “bailout” for coal-fired power plants.

- A protester opposed to Kinder Morgan’s activities on Burnaby Mountain in Canada is taking the corporation to court. The activist claims he is defending his right to protest, and hopes the case inspires the province to reintroduce legislation barring SLAPP suits.

- U.S. Senator Charles Schumer is pushing federal regulators to expedite their rulemaking on DOT-111 train cars still being used to transport highly volatile crude oil across New York State. The train cars could potentially put local communities in danger given they are prone to rupture and explode during derailments.
The Denver Post reports: Speaking to reporters outside the White House, Colorado Gov. John Hickenlooper said Tuesday afternoon that he supported the administration’s pledge to veto new legislation from Congress that would fast-track construction of the controversial Keystone XL pipeline. Earlier in the day, Josh Earnest, the White House press secretary, confirmed that President Barack Obama would veto a pro-Keystone XL measure that new Republican majorities in Congress have made a top priority at the start of the latest session. Hickenlooper said Obama, a fellow Democrat, was making the right call in opposing the U.S.-Canada oil pipeline.

On Tuesday, the White House stated that President Obama would veto legislation approving construction of the Keystone XL pipeline. “If this bill passes this Congress the president won’t sign it,” White House press secretary Josh Earnest said.

Agribusiness

The leader of the largest U.S. farm organization said GMO food labeling, debated at the state level for the past three years, would result in “patchwork regulation that will do nothing but raise the cost of food.”

“Four animal activists who took pictures of a large southwestern Utah hog farm pleaded not guilty” to violating a state law against entering agricultural property in order to take photographs, says Feedstuffs. The four, from California and Maryland were charged with trespass and agricultural operation interference at the Circle Four Farms near Milford, Utah, which is owned by a subsidiary of Smithfield Foods. A lawyer for the group said they were on a public road and took photos of buildings, rather than animals or workers. The Salt Lake (City) Tribune says the group “may be the first defendants prosecuted under Utah's 'ag gag' law.”

Nearly three dozen farm groups and agribusinesses announced a joint effort as the U.S. Agriculture Coalition for Cuba “that seeks the end of the U.S. embargo on Cuba and to advance trade relations between both nations. The USACC seeks to advance trade relations between the U.S. and Cuba by re-establishing Cuba as a market for U.S. food and agriculture exports.”

While urban America has nearly universal access to wired broadband, the rate in rural America is 78 percent, according to industry data. USDA’s 2012 Census of Agriculture says 70 percent of farms have Internet access but a third of them use dial-up, satellite or mobile connections "that may not be adequate when it comes to accessing and delivering the large quantities of data that are associated with some precision agriculture processes," write Brian Whitace, Tyler Mark and Terry Griffin in Choices, the journal of agricultural economics. "The availability of broadband for farm offices and land in production has serious implications for the future of agriculture."

Thirty countries, including Canada, Mexico and Japan, have imposed restrictions or a total ban on imports of poultry from the U.S. Northwest following discovery of a highly pathogenic avian influenza in Oregon and Washington state last month.

Ireland is the first European country to regain access to U.S. sales following removal of trade restrictions put in place against mad cow disease 15 years ago.

Seed companies such as Scotts Miracle-Gro and Callectis Plant Sciences are utilizing techniques to genetically modify crops that are outside of federal jurisdiction or use methods that were not imagined when the regulations were created, said the New York Times.

TwinCities.com reported that a California apple packing plant has recalled all of its Granny Smith and Gala apple shipments from 2014 after they were linked to an outbreak of listeria in caramel apples that may have caused up to five deaths, including two in Minnesota. Six people have died in a multi-state outbreak of Listeria monocytogenes illnesses linked to caramel apples, the US Centers for Disease Control and Prevention (CDC) has reported.
• The Boston Herald reported that a Massachusetts couple has filed suit against Whole Foods Market and a Missouri beef supplier, alleging its E. coli-contaminated beef caused the death of the couple’s eight-year-old son. The suit seeks unspecified damages.

• Food Production Daily reported that Tyson Foods has begun the New Year by getting its manufacturing operations in shape. The US’s second-largest food processor recently concluded a line expansion at its prepared foods plant in Emporia, Kansas and put its Buffalo, New York facility up for sale.

• Food Production Daily reported that a coalition representing more than 30 agricultural organizations and companies to deepen US-Cuba trade relations held a press conference (January 8) to mark its official launch.

• The Wall Street Journal reported that General Mills Inc. said it plans to eliminate another 500 jobs with the closures of two Pillsbury dough factories, adding to the roughly 1,400 job cuts it announced last year as it tries to improve profitability amid lackluster industry sales.

• U-T San Diego reported that Petco said Monday it has removed all remaining Chinese-made dog and cat treats from its website and stores nationwide because of concerns they have sicken thousands of pets and killed 1,000 dogs in the U.S. since 2007.

Insurance/Healthcare

• The rapid rise in cyber-attacks on healthcare organizations necessitates the use of a cyber-centric framework. Recent incidents, including the hacking attack on Community Health Systems, show healthcare is an easy target.

• The cyberthreat that is front and center for many healthcare information security leaders these days appears to be their business associates. At least that’s what respondents have been indicating so far in HealthcareInfoSecurity’s fourth annual and ongoing Healthcare Information Security Today survey.

• The Office of the National Coordinator for Health IT, the unit of the Department of Health and Human Services that oversees policy and standards for the HITECH Act electronic health record financial incentive program, later this month expects to release a final draft of a "10-year roadmap" that includes an emphasis on the interoperability of EHR systems, paving the way for nationwide secure health data exchange.

• The biggest 2014 U.S. health data breaches listed on the federal tally so far demonstrate that security incidents are stemming from a variety of causes, from hacker attacks to missteps by business associates.

• Beginning in early 2015, the Office for Civil Rights’ plans to audit 200 covered entities, including healthcare providers and group health plans, to measure their compliance with the HIPAA privacy, security, and breach notification rules requirements. These audits of covered entities will be followed by up to 400 audits of business associates to measure their compliance with the security rule and how they intend to approach their obligations under the privacy and breach notification rules.

• With the healthcare sector becoming a growing target for cybercriminals, it’s critical that organizations implement information security management practices that go far beyond a focus on HIPAA compliance. Yet, one of the biggest mistakes many healthcare entities continue to make in protecting patient information from cybercrime is taking a compliance-centric approach to information security.
Financial Services

Activism

- Housing activists held a protest at a property management office in Atlanta, GA on January 6, 2015 in support of a local homeowner who was evicted from her home in December 2014. The homeowner has since re-occupied her former home and claims that a leading U.S. bank unlawfully foreclosed on the house.

- Unions in the Indian banking sector on January 6, 2015 decided to defer their January 7th planned national strike with the Indian Banks’ Association (IBA), upping its wage hike offer by 1.5% to 12.5%. The United Forum of Bank Unions (UFBU) threatened to go on strike January 7th followed by four days of continuous strikes January 21-24th and an indefinite strike from March 16th demanding early resolution of their wage hike talks.

- A Northern California coalition dedicated to getting big money out of politics will conduct a march and rally on January 21, 2015 in San Francisco, CA to protest the 5th anniversary of the Citizens United decision by the Supreme Court to “empower Big Money over the People.” The event is sponsored/endorsed by numerous other activist groups.

- An Indian student activist group conducted a protest on January 6, 2015 at the Department of Finance in New Delhi, India. Participants protested the Ministry of Finance and IBPS’ (Institute of Banking Personnel Selection) road map for “huge job cuts” in banks and “unethical profiteering” by private Institutions.

- Occupy Wall Street will continue to conduct police brutality “die-in” actions every Monday at Grand Central Terminal in NYC starting at 7:00pm EST.

- Housing activists will conduct a rally on February 7, 2015 in Washington DC to bring attention to diverse neighborhoods and “housing opportunities for everyone.”

- Protests against Canada’s “failed” governmental systems will occur in various cities throughout Canada on February 13, 2015. Participants are encouraged to blockade their local railway, port or highway.

- Anti-foreclosure activists are organizing a clandestine action against an Atlanta, GA-based mortgage loan servicing company for perceived mortgage and loan modification abuse.

Information Security Risk

- A hacker released a tool that he says can break into any account of a popular cloud service developed by a leading IT company headquartered in Cupertino, California. The tool, iDict, uses an exploit in the company’s security to bypass restrictions that stop most hackers from gaining access to accounts. The tool is described as a 100% working ID dictionary attack tailored to the company’s cloud service that bypasses account lockout restrictions and secondary authentication on any account.

- Hackers known for their blackmailing techniques launched a new website which holds an archive of their latest hacks on companies which declined to pay their ransom demands.

- A new study showed a total of more than 61 million retail records were stolen, lost or leaked in the United States last year, which is less than the over 70 million records compromised in 2013.

- A Mountain View, CA-based search engine company closed the details of an unpatched Windows vulnerability reported to Microsoft in September 2014. The disclosure was made on January 5, 2015 upon the expiration of 90-day waiting period imposed by the Internet giant. Microsoft has yet to patch the Windows 8.1 vulnerability that would allow a hacker to elevate their privileges on an affected computer to gain administrator access. Microsoft’s next set of Patch Tuesday security bulletins are scheduled to be released January 13, 2015. The Mountain View company said the
NtApphelpCacheControl system call, which allows for quick caching of application data, contains a vulnerability in which a user’s impersonation token is not checked properly to determine if the user is an administrator.

- A Finnish bank last week suffered a cascading series of distributed denial of service (DDoS) attacks that began on New Year’s Eve. The bank was forced to restrict access to its services from outside the Nordic country as a result of the attack. The company said in a press release that traffic in the denial of service attack originated both inside and outside Finland.

- Experts warned that hackers are increasingly focusing their phishing campaigns against bank employees, rather than bank customers. Hackers are targeting banking institution employees with convincing e-mails that fool them into clicking on malicious links - which ultimately compromise their credentials or other sensitive information - or trick them into providing details about accountholders and their accounts. This information is often used by hackers to take over customers’ accounts to perpetrate fraud.

- A leading U.S. investment firm fired one of its financial advisers after it accused him of stealing account data on about 350,000 clients and posting some of that information for sale online, in potentially the largest data theft at a wealth-management firm.

- India’s central banking institution is considering removal of its two-factor authentication requirement for small-value transactions up to Rs. 3,000 (roughly $47 USD). The stated goal is to facilitate easier electronic transactions for consumers. Security experts, however, fear the initiative may actually increase fraud.

- A UK- and Slovenia-based bitcoin exchange announced on January 5, 2015 that it would be going offline while it investigated a security compromise of some portion of its stored currency that occurred over the weekend. According to a message on its homepage, the company noted that one of its operational wallets was compromised on January 4, 2015, and subsequently suspended its service. Less than 19,000 BTC (worth about $5 million; one BTC is about $270) was stolen.

- The Dridex banking malware is being used in malicious spam campaigns that are generating 15,000 emails per day. The attacks, largely against users in the United Kingdom, are leveraging macros in Microsoft Office documents to infect users. The way the attack works is that a user receives an infected Office document that includes a macro that triggers a download of the Dridex banking malware. Dridex steals user banking information and attempts to generate fraudulent financial transactions. Two recent macro downloaders that spread through spam email campaigns are TrojanDownloader:W97M/Adnel and TrojanDownloader:O97M/Tarbir.

- Hackers claimed to have compromised the servers of a Swiss bank and downloaded 30,192 private emails sent by both Swiss and foreign customers, in addition to various other “interesting data.”

- An undisclosed number of individuals who used their credit cards to book reservations through the website of an international hotel management company may have had their personal information compromised. The company began receiving calls from customers regarding suspicious activity on their credit cards, and investigators identified activity in the company system that possibly indicates unauthorized access to the personal information. The compromised information includes names, addresses, credit card information, telephone numbers, email addresses and possibly dates of birth.

- Researchers warned that a new variant in the Win32/Emotet family is targeting banking credentials with a new spam email campaign. The emails include fraudulent claims, such as fake phone bills, and invoices from banks or PayPal. This campaign primarily targets German-language speakers and banking websites.

- A known hacker group leaked financial sector documents to an open source paste site on January 9th, further indicating that more file dumps will be disclosed in the future.

Legal, Litigation, Regulatory Risk
• A leading bank in Scotland may have to pay as much as £5 billion ($7.7 billion) to settle charges against it for selling toxic mortgage-backed securities to the two GSEs for housing.

• The UK’s major banks warned that new rules designed to “ring-fence” their retail operations to protect consumers could mean tens of millions of people being forced to change sort codes. A leading trade association, which lobbies on behalf on the UK’s banks, said the Bank of England rules, which will force the legal separations of high street banks from investment banking operations, could disrupt payment systems if the banks are not given enough time to deal with the issue. The group, in its submission to a consultation on the reforms, called for the Bank to finalize the rules before the expected deadline of the first half of 2016.

• A leading U.S. bank announced it will take a $145 million charge against its fourth-quarter earnings for legal expenses related to a federal inquiry into its handling of problem mortgages and foreclosures. In a U.S. Securities and Exchange Commission (SEC) filing, the Atlanta-based bank said the cost will reduce its fourth-quarter earnings by $0.17 per share. The bank said the expense is related to resolving one issue in its “previously disclosed legacy mortgage matters.”

**Operational Risk**

• A new ATM scam known as a “black box” attack is draining ATM cash deposits across the country. In a black box assault, the criminals gain physical access to the top of the cash machine. From there, the attackers are able to disconnect the ATM’s cash dispenser from the “core” (the computer and brains of the device), and then connect their own computer that can be used to issue commands forcing the dispenser to spit out cash. Researchers note that black box attacks are one of two “logical” attacks seen so far against ATMs. The other type of logical attack uses malicious software that similarly “jackpots” the cash machine, forcing it to spit out cash. In both cases, the attacks are made possible because thieves are able to physically access the top part of the ATMs where the USB ports are located. To help prevent the type of physical access that allows thieves to perpetrate logical attacks, researchers urge customers who plan to deploy cash machines in unattended areas to consider wall-mounted units as opposed to stand-alone units.

• An article reported that pressure is growing to split up a NYC-based financial institution, which is the largest US lender by assets and the world’s biggest investment bank. A leading U.S. investment firm published an equity research note arguing that the bank should be broken into pieces because its parts are worth more than the whole. The article added that regulators have proposed tougher rules penalizing companies for size and complexity.

**Reputational Risk**

• The Bank of England’s senior executives are accused of being guilty of “groupthink” and complacency in the run-up to the country’s credit crisis in 2007, and even in the months after a leading retail mortgage lender was rescued. The minutes of monthly meetings between June 2007-09 of the Bank of England’s board – or Court – which included some of the best-known figures in U.K. business as its non-executive directors, were made public following a disclosure campaign. According to the article, they show what has been described as a general failure to grasp the danger facing the U.K. banking system in the run-up to the global financial crisis.

• Two U.S. churches filed a lawsuit against a leading U.S. bank for “self-dealing.” The churches claim the bank, entrusted to manage funds to support the churches’ “good works,” put its own financial interests first. Their claims came after other religious orders pressed the bank for a report on its business standards, prompting it to release almost 100 pages last month describing its efforts to bolster ethics and compliance.
Brazil

- O Estado de S. Paulo reports that the Brazilian Auto Industry lost 12,400 jobs in 2014, the highest since 1998.

- The Financial Times reported that Brazil is about to attempt pension reform. Brazil’s pension system has long struggled with one particular problem: “sugar daddies”, or more precisely, the situation where young women marry men old enough to be their grandfathers so they can lay claim to their pensions when they die. This is about to change.

- Bloomberg reports that the 2016 Rio de Janeiro Olympics may feature two more soccer venues because of concern over the ability of fields to cope with multiple games through the preliminary rounds. The decision will be a boon to cities with world cup quality stadiums without major teams to support them.

- Veja reports that Friday evening protests over bus fare hikes by 7,000 people in downtown in São Paulo degenerated into rioting reminiscent of the June 2013 protests where masked vandals broke windows, burned vehicles, and looted in many cities across the country. 51 were arrested.

China

- A lower level police department in Wenzhou was left red-faced when it emerged that officers had spent 149,000 yuan ($24,000) buying a device and software designed to plant Trojans into phones to monitor its own citizens. China is already thought to pay tens of thousands of people to post pro-government comments on Web sites and social media; they are known as the Fifty Cent Party, after the amount of money (0.5 yuan or 8 U.S. cents) they are thought to receive for each post.

- A Chinese security news outlet reports a security vulnerability on wireless routers that use admin/admin as username/password could be exploited by embedding a malicious webpage. Once users visit the malicious page, the router's DNS IP address will be modified, and personal information like banking information could be obtain.

- A Chinese cyber security website reports 8 Network Time Protocol security vulnerabilities. The most serious vulnerability (CVE-2014-9295) could allow an attacker to gain remote access with just one packet.

- A Chinese website reports the high risk security vulnerability on U-Mail reported in May 2014 still exist and it is a potential threat to governmental and corporate confidential information.

- A Chinese news outlet reports police force in Wenzhou province, China public purchased trojan malware to monitor Android and iPhone users phone conversation. According to the article, the malware is specialized in targeting rooted Android devices and jailbroken Apple devices.

- In a January 8, 2015 posting on Sina.com.cn reports a popular train ticket grabbing application contains a high risk security vulnerability that exposed users sensitive information.

- Posting on Xinhuanet.com reports the security risk of use public free Wi-Fi in China.

- A article on 163.com reports a high risk security vulnerability on China Unicom, a major telecommunication operator in China. According to the article, the vulnerability could be exploited by targeting user's phone number and obtain user call log, message log, location and logged in social media accounts.

- China Tech News reported that Microsoft announced that they will formally shut down manufacturing plant in Beijing and Dongguan in the first quarter of 2015, which will cost over 1,000 jobs. Microsoft officially informed employees in the two factories on December 17, 2014, and the company plans to complete the adjustment in the first quarter of 2015. Compensation plan provided by Microsoft is “N+2” and year-end awards. N equals to the years of service in the two factories. Employees from the two factories revealed that Microsoft asked them to sign the agreement by January 6,
2015. If the employees do not accept the agreement, Microsoft will unilaterally terminate the labor contract and pay compensation based on legal standards. Many employees reportedly cannot accept the compensation plan and are implementing negotiations with Microsoft. However, their demand for more compensation has not yet received any response.

Germany

- Hacker network Anonymous posted multiple messages declaring websites associated with the German PEGIDA movement as possible targets for cyber-attacks. Some websites thought to associated with PEGIDA or sharing its political view were already subjected to defacement and DDoS attacks. PEGIDA, which stands for Patriotic Europeans Against the Islamization of the West, is a German right-of-center protest movement criticizing European and German immigration policies. Recent rallies saw thousands of protestors, a large rally in Dresden on Jan. 5 in Dresden drew around 18,000 participants. The rallies also spark large counter-protests. A possible impact from last week’s terror attacks in Paris remains to be seen.

India

- Business Standard reported that India’s Tamil Nadu police arrested 194 workers of FIH India, formerly known as Foxconn India, when they tried to enter the premises of the company’s Sriperumbudur plant on 1/5/2015, said E. Muthukumar, president of Foxconn India Employees Union. The factory remains closed since December 22, 2014 owing the lack of orders. The company has also said to will offer voluntary retirement scheme or severance package to employees.

Israel

- Globes reported that Israel’s attorney general Yehuda Weinstein has given the final approval for passing legislation agreed on by state and Histadrut (General Federation of Labor in Israel) representatives raising minimum wage to NIS 5,000 in three installments during the election campaign. The minimum wage will be raised to NIS 4,650 on April 1, 2015, NIS 4,825 on July 1, 2016, and NIS 5,000 on January 1, 2017.

North America

- SFGate reported that Intel is shaking up Silicon Valley by taking serious steps to overcome the lack of diversity in its job ranks. Intel CEO Brian Krzanich pledged that his company will spend $300 million by 2020 to widen its hiring and improve the company's employment diversity profile.

- Jacksonville reported that decades after a federal banned discrimination against pregnant women in the workplace, some states are providing additional protections to pregnant workers who want to stay on the job. It's illegal under the federal Pregnancy Discrimination Act to fire a worker, cut her pay or deny her health benefits because she is pregnant. But the law applies only to employers with 15 or more workers and is unclear on the extent to which employers must accommodate pregnant employees so they can continue to work. Pregnancy alone is not a disability under the federal Americans with Disabilities Act, although it does protect women with pregnancy-related impairments, such as difficulty bending or lifting heavy objects. Courts have tended to rule narrowly on what employers must do to accommodate pregnant workers, and women’s rights advocates contend that many pregnant women are pushed out of their jobs. As of Jan. 1, employers in Illinois must provide pregnant workers who request them more or longer bathroom breaks, rest periods, light duty, job transfers, leave time or other accommodations, unless doing so creates an undue hardship for the employer. Eleven other states have passed laws requiring employers to provide reasonable accommodations to pregnant workers. In 2014, laws took effect in Delaware, Minnesota, West Virginia and the District of Columbia. Since 2011, Alaska, Connecticut, Maryland and New Jersey also have approved laws.

- Farhang & Medcoff reported that On 12/11/2014 the National Labor Relations Board (NLRB) issued its decision in Purple Communication, Inc., 361 NLRB 126 (2014) holding that Section 7 of the National Labor Relations Act (NLRA) requires employers – even non-unionized employers—to allow employees, during non-work time, to use corporate e-mail systems for union organizing communications and/or to discuss terms
and conditions of employment. The 3-2 decision overturned the Board's prior decision in Register Guard, 351 NLRB 1110 (2007), which had held that corporate e-mail systems are property of the employer, which could ban or regulate, in a non-discriminatory manner, all non-business (including union-related) e-mail communications.

Vietnam

- Lao Dong News reported that workers from Carmax Sai Gon have been on strike since January 3, 2015 to demand for increase in wages. Company leaders have announced that the workers have been on strike over the legal number of days they are allowed to strike and the company has proceeded to lay off these workers. Company leaders have also stated that they intend to sue these workers for company lost due to the strike. The company stated that before they pursue legal options, the company will “help” workers who agree to wage conditions and Lunar New bonuses proposed by the company, the company will “agree” to protect workers to avoid them from being sued and help them return to work so that workers will not encounter any problems.

- On January 7, 2015 the Independent reported that the underwater trans-Pacific cable that provides internet to much of Southeast Asia saw the latest in a series of ruptures that have blighted Vietnam and other countries in recent months, causing millions to experience slow or intermittent connections. While previous theories have included foul play and snagging by anchors, the reason behind the breakages is increasingly thought to be sharks chomping down on the cables.

- On January 7, 2015 Yahoo! News reported that Vietnam’s central bank said it would devalue the Vietnamese dong currency for the second time in seven months in a bid to boost exports and drive economy forward. The State Bank of Vietnam (SBV) will devalue the reference rate by one percent to 21,458 Vietnamese dong per dollar to "control inflation" and "push up economic growth", it said in a statement. The dong was last devalued by one percent in June 2014.

Legal and Regulations

- On December 16, 2014, the Conference of State Bank Supervisors (“CSBS”) issued a Policy on State Regulation of Virtual Currency (the “Policy”), Draft Model Regulatory Framework, and a request for public comment regarding the regulation of virtual currency. The Policy and Draft Model Regulatory Framework were issued through the work of the CSBS Emerging Payments Task Force (the “Task Force”). The Task Force was established to explore the nexus between state supervision and the development of payment systems and is seeking to identify where there are consistent regulatory approaches among states.

- The FCC plans to continue pursuing privacy actions against telecommunications companies with lax data security practices, according to a letter sent by FCC Chairman Thomas Wheeler. In response to feedback from Sen. Bill Nelson (D-FL), who lauded the FCC’s first-ever data security enforcement action against two phone companies - YourTel America Inc. and TerraCom Inc. - Wheeler affirmed that the FCC will “exercise its full authority” to hold companies liable under the Communications Act for failing to protect customer data.

- The International Standards Organization’s new cloud standard, ISO 27018, strives to ensure that public cloud service providers (such as Amazon, Google, and Rackspace) “offer suitable information security controls to protect the privacy of their customers’ clients” by securing the personally identifiable information (PII) entrusted to them. The new standard, adopted by ISO and the International Electrotechnical Commission in August, is voluntary. It is expected to be followed by ISO 27017, which will cover non-privacy information security aspects of cloud computing. According to the ISO, the new standard is intended as “a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system ….” Broadly, ISO 27018 addresses the questions of confidentiality and security of the customer’s personal information and the prevention of its unauthorized use.
California S.B. 568, titled "Privacy Rights for California Minors in the Digital World," (the "Privacy Law") took effect January 1, 2015. The new Privacy Law includes a provision known as the "Eraser Law" that gives California minors a right to delete content that they posted to a website, social media profile, or online service while under the age of 18. The Privacy Law also includes restrictions on marketing or advertising certain enumerated products and services to minors.

California recently passed a new law that makes it unlawful to include nondisparagement clauses in consumer contracts. Nondisparagement clauses generally restrict individuals from making statements or taking any other action that negatively affects an organization, including its reputation, products, services, management, or employees. The new law, codified at California Civil Code section 1670.8, which took effect January 1, 2015 specifically provides that "a contract or proposed contract for the sale or lease of consumer goods or services may not include a provision waiving the consumer’s right to make any statement regarding the seller or lessor or its employees or agents, or concerning the goods or services."

Worldwide

In May 2014, Court of Justice of the European Union ("CJEU") delivered the ground-breaking "Google Spain" ruling, which recognises the right for individuals to have links about themselves de-listed from search results. In response to the complaints received, the Article 29 Working Party (Art 29 WP) published a report on work being carried out to handle complaints, and the European Commission (Commission) published a report dispelling myths on the "rights and wrongs of the so-called right to be forgotten". The reports illustrate how the "right to be forgotten" has been widely misinterpreted, and they seek to create widespread understanding of the judgment, including clarifying the extent of EU citizens’ rights. While clarifying the scope of the right, the Art 29 WP also complicated matters for search engines by stating that the right applies globally, not just to EU-related domains, such as .co, .uk or .es.

Pharmaceuticals

Concerned over surprise inspections by the FDA, the Indian government has asked the agency to allow its own regulators to attend inspections of domestic facilities.

In their latest bid to lower prescription drug costs, two U.S. Senators have re-introduced legislation that would allow Americans to purchase medicines from Canada. This marks the second consecutive year that Amy Klobuchar (D-Minn.) and John McCain (R-Az.) have advocated the Safe and Affordable Drugs from Canada Act. The bill would permit Americans, who must have a valid prescription from a physician licensed in the U.S., to order up to a 90-day supply of medicines from a licensed Canadian pharmacy.

China will allow online sales of prescription drugs as early as this month, a policy that will open up an over 1 trillion yuan ($161 billion) market to online pharmacy operators like Alibaba Group Holding Ltd and Wal-Mart Stores Inc.

Retail

J.C. Penney said Thursday it will close about 40 stores over the next year. The closures, which represent nearly 4 percent of the 1,060 Penney U.S. stores, will affect about 2,250 employees, according to spokesman Joey Thomas.

On Sunday, Crayola’s Facebook page was hacked by unknown deviants. Once inside the brand's account, the perpetrators shared click-baity links to R-rated sites throughout the day, sending Crayola into a panic.

President Obama today will propose the first federal standard for data breaches,
requiring companies to notify customers within 30 days of the discovery that their personal information was exposed to hackers.

- Online retailer Zappos this week settled with attorneys general in nine states, agreeing to pay out $106,000 stemming from a data breach in 2012 that exposed 24 million customers' information.

- Coca-Cola said it plans to layoff approximately 1,600 to 1,800 employees globally in the next few months in an effort to cut costs.

- Teen retailer Wet Seal announced it will close 338 stores. The decision was based on its overall financial condition and an inability to negotiate meaningful concessions from its landlords.

- Cincinnati.com reported that Macy's plans to restructure its merchandising and marketing and lay off of thousands of workers in response to changes in the way customers shop in stores and online. The retailer said Thursday it will also close 14 department stores but open two new locations, resulting in annual savings of roughly $140 million. Macy's says it plans to reinvest those savings into its business.

- The Sun Times reported that Ace Hardware Corp. has bought a hardware distributor with business in 11 western states. Oak Brook-based Ace Hardware said Tuesday it has acquired Jensen Distribution Services, a 131-year-old company based in Spokane, Washington. Jensen, with about $150 million in wholesale revenue, serves more than 2,000 customers.

- According to findings from IBM, the number of cyber attacks against US retailers has declined 50%, however, the number of records stolen from them remains at near record highs. Contrary to expectations, cyber attackers scaled back on Black Friday and Cyber Monday 2014 hacking efforts.

- CBS News reported that Dunkin' Donuts confirmed Wednesday that it struck a deal to open more than 1,400 locations in China over the next 20 years.

- The Chicago Tribune reported that McDonald's said it is laying off 63 people at its headquarters in Oak Brook, where it employs about 1,700 people. Those layoffs are set to start in February. McDonald's cuts are among 600 layoffs expected in coming months at Illinois companies that filed advance warning reports with the state.

---

**Technology**

- Gmail has been blocked in China. Anti-censorship and privacy advocates speculated on filtering activity operated by the national Great Firewall system.

- New research out from the GlobalWebIndex indicates that in a survey of 170,000 adult Internet users across 32 markets, only 9% report having a smartwatch, and 7% said they owned smart wristbands. In contrast, among online adults, 80% now own a smartphone.

- In a joint statement put out yesterday, the justice and interior ministers of 12 European countries — including the U.K., France and Germany — express concern at “the increasingly frequent use of the Internet to fuel hatred and violence and signal our determination to ensure that the Internet is not abused to this end”. They also call for major ISPs to partner with governments to enable “swift reporting of material that aims to incite hatred and terror and the condition of its removing, where appropriate/possible”.

---

**Telecommunications**
A group of Democratic leaders have incited a new political debate over what direction net neutrality should take by reintroducing a bill that would put a ban on paid prioritization agreements between content providers like Netflix and ISPs like AT&T and Verizon.

The Australian government signaled on Monday its determination to press ahead with legislation forcing telecommunications companies and internet service providers (ISPs) to store customer details known as metadata for two years, although key details such as costs and technical requirements are yet to be settled.

The Federal Communications Commission will decide on a new set of rules that might increase regulation on ISPs next month. Under new regulations, the FCC would have more transparency over deals like ones with Netflix and could set rates that Internet providers can charge for them.

Entertainment

The FBI revealed more details related to the Sony investigation. It claims that messages sent by the attackers were detected and showed that they were IP addresses only used by North Korea. Some experts still believe Sony employees may have been the culprits, whether it was an isolated incident or a joint effort with North Korea.

Defense

Hackers claiming to be aligned with Islamic State militants took control of the U.S. Central Command’s Twitter and YouTube accounts Monday, posting phone numbers of top military officers and what they said were classified documents.

More nation states will build elite cyber espionage teams, with the big players being the U.S., U.K., China, Russia, and Israel.

U.S. suspects North Korea's surveillance body was involved in Sony cyber-attack using an internet protocol address in Shenyang. The source said a hacker who is already identified as engaging in activities under the bureau was confirmed to have been handling data via the IP address, including email threats to Sony Pictures executives.

The Department of Homeland Security and Department of State have launched the next stage of an aggressive campaign to make clear the national security, border security, and public safety priorities that are now in effect, and to clarify the criteria for filing requests for deferred action under the Executive Actions recently announced by President Obama.

Law Enforcement

France's government urged the nation to remain vigilant Saturday, as thousands of security forces try to thwart new attacks and hunt down a suspected accomplice in a rampage by terrorists linked to al-Qaida in Yemen that scarred the nation and left 20 dead.

French law enforcement officers have been told to erase their social media presence
and to carry their weapons at all times because terror sleeper cells have been
activated over the last 24 hours in the country, according to a French police source.
Amedy Coulibaly, a suspect killed Friday during a deadly kosher market hostage siege,
had made several phone calls about targeting police officers in France, according to
the source. It was also reported in a French-language magazine that brothers Cherif
and Said Kouachi had been under watch by the French, but despite red flags,
authorities there lost interest in them.

- A former college student imprisoned since a jury convicted him of eco-terrorism in
2007 was freed Thursday after it was discovered the FBI and prosecutors withheld
thousands of pages of evidence that could have been used for his defense. Federal
prosecutors realized they had little choice but to support the release of 37-year-old Eric
Taylor McDavid, prompting a judge Thursday to order his release. McDavid was in
prison for allegedly plotting to bomb the Nimbus Dam, cell phone towers and a U.S.
Forest Service lab.

- Airport and airline employees will soon face tougher security measures being
implemented by the TSA. Homeland Security made the announcement just weeks
after a gun-smuggling operation in which a bag handler and ramp agent were involved.
Among the potential security measures could be airline-employee screenings,
aditional TSA patrols and random security checks.

- FBI Director James B. Comey said on Wednesday that he has no doubt that North
Korea was behind the devastating cyber-attacks on Sony Pictures. Comey said the
hackers were easily traceable because they made a critical error by failing to conceal
their location, sending messages and attacks from North Korean Internet addresses.
More sophisticated hackers would have routed their attacks and messages through
decoy servers – something the hackers tried to do after realizing they were using their
country's Internet addresses, Comey said.

- Police Departments across the nation are responding to a threat from ISIS with
increased vigilance after someone re-released a September 2014 message that tells
followers to "rise up and kill intelligence officers, police officers, soldiers, and civilians."
The threat specifically named the United States, France, Australia and Canada as
targets.

- Staff members at a Colorado NAACP office say they are waiting for more information
before drawing conclusions about an explosion near their chapter, even as the FBI
investigates whether the blast was domestic terrorism. "We're exploring any potential
motive, and domestic terrorism is certainly one among many possibilities," Denver FBI
spokeswoman Amy Sanders said. An improvised explosive device was detonated
about 11 a.m. Tuesday outside a barbershop that shares a building with the NAACP
chapter, but a gasoline canister placed next to the device failed to ignite. There were
no injuries and only minor damage to the building, which sits in a mostly residential
neighborhood.

- Following the recent deaths of several NYPD officers, Chuck Canterbury, National
President of the Fraternal Order of Police, has once again called on Congress to
expand the Federal hate crime laws to protect law enforcement officers. The FOP has
advocated for more than a decade to expand Federal protections for law enforcement
by increasing the penalties on perpetrators who select their victims because they are
or are perceived to be police officers.