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.

LEARN MORE

Top Incidents

Energy

- Legislation to approve the controversial Keystone XL oil pipeline began racing through the U.S. Congress on Wednesday as Democrats and Republicans appeared to be coming together in a challenge of President Barack Obama’s oversight of the project. In a series of rapid developments that unfolded just hours after Congress returned from a seven-week recess, there were indications the measure could pass and be sent to Obama in the coming weeks.

Agribusiness
A dozen farm groups and agribusinesses agreed on a 10 principles for data privacy and security in the emerging field of agricultural Big Data. They include an assurance that technology companies will not use farm data to speculate illegally in commodity markets. Other guidelines say farmers own the information generated on their land, that farmers can retrieve their data from technology companies, that companies will disclose if they share farm data with others, and companies will protect the privacy of the data.

Insurance/Healthcare

- Healthcare data encryption is becoming an increasingly hot topic, especially as more providers implement EHRs and work to develop strong BYOD policies across their organizations. No one wants to make headlines for a healthcare data breach, especially if the cause was easily avoidable. By making sure that data is encrypted when it is stored locally on devices – data at rest – and when it is sent from one device to another – data in motion – healthcare organizations can ensure that patients’ protected health information (PHI) is safe from unauthorized users.

Financial Services

- Chinese government hackers are suspected of breaching the computer networks of the United States Postal Service, compromising the data of more than 800,000 employees. The intrusion was discovered in mid-September.

Global Intelligence

- A Chinese security news outlet reports a malware targeting Android devices caught on November 11, 2014, hence dubbed as “Double-11 SMS Thief”. The malicious Trojan are able to disguise as an application associated with China Mobile and lure users to download. Once installed, the malwares are able to intercept text message contains online bill pay information and banking information.

Legal and Regulations

- In an effort to push retailers to adopt heightened security for credit and debit cards, President Barack Obama signed an executive order mandating chip-and-PIN technology for government cards. While the order applies only to government-issued cards and card terminals, the President took the opportunity to urge all stakeholders to “drive the economy towards more secure standards to safeguard consumer finances and reduce their chances of becoming victims of identity theft – America’s fastest growing crime.”

Pharmaceuticals

- The United States Department of Justice Antitrust Division (DOJ) recently served two U.S.-based generic pharmaceutical manufacturers with criminal grand jury subpoenas. It is reported that the subpoenas request all communications discussing generic pharmaceutical pricing and sales with competitors, and that they are not limited to particular products. The subpoenas signal a much broader federal investigation into potential Sherman Act violations in the generic pharmaceutical industry—with potential criminal implications for the companies and individuals involved. It is unusual that the DOJ, and not the Federal Trade Commission's Bureau of Competition (FTC), is investigating this industry and certainly significant that the DOJ issued criminal grand jury subpoenas to do so.

Retail

- Germany's foreign intelligence agency plans to spend millions to penetrate the secure connection technologies used by social networks, banks and online shops.

Technology

- The Wall Street Journal published a report claiming that the U.S. Justice Department is
“snagging [mobile data belonging to] a large number of innocent Americans” via technology that can identify criminal suspects using planes. The WSJ cites sources who claim that the U.S. Marshals Service is using fake cell towers on airplanes — dubbed ‘dirtboxes’ — in order to access data from phones located on the ground.

**Telecommunications**

- Net Neutrality advocates blockaded the driveway of FCC Chairman Tom Wheeler in protest of the FCC’s anticipated ruling on the matter. The advocates claim that Mr. Wheeler is not representing the public and that he is working for companies like Verizon and AT&T, as the protesters cite Wheeler’s prior experience to FCC as a lobbyist for cable and telephone corporations.

**Entertainment**

- Brooklyn Nets fans trying to locate the team’s schedule or recent score may have typed “nets.com” into their browser and been redirected to a variety of sites unrelated to the team. The Nets do not own the domain Nets.com and the rightful owner has been playing tricks on the team’s fans with their antics.

**Defense**

- The State Department has taken the unprecedented step of shutting down its entire unclassified email system as technicians repair possible damage from a suspected hacker attack. A senior department official said Sunday that activity of concern was detected in the system around the same time as a previously reported incident that targeted the White House computer network. That incident was made public in late October, but there was no indication then that the State Department had been affected.

**Law Enforcement**

- From Boston to Los Angeles, police departments are bracing for large demonstrations when a grand jury decides whether to indict a white police officer who killed an unarmed black teenager in Ferguson, Missouri. The St. Louis County grand jury, which has been meeting since Aug. 20, 2014 is expected to decide this month whether Officer Darren Wilson is charged with a crime for killing Michael Brown after ordering the 18-year-old and a friend to stop walking in the street on August. 9, 2014. The shooting has led to tension with police and a string of unruly protests there and brought worldwide attention to the formerly obscure St. Louis suburb, where more than half the population is black and yet few police officers are.

**Energy**

- A National Summit for a Nuclear Free Future was hosted by the Sierra Club November 14-17, 2014 in Chevy Chase MD. The summit was attended by activists who are working to end nuclear power and all of its related industries.

- Activists staged a “Stop the Pipeline Statewide Summit” in Fitchburg MA on November 15, 2014. The crowd of several hundred people rallied against a proposed natural gas pipeline by Kinder Morgan which would traverse properties from New York to New Hampshire.

- Activists staged a demonstration and placed flyers on employee vehicles parked at Suncor’s Sarnia Ontario refinery in continued protest of the company’s plans to erect 46 wind turbines in Lambton County. The group has requested that the company not proceed with any construction until all legal challenges have been completed.

- Legislation to approve the controversial Keystone XL oil pipeline began racing through
the U.S. Congress on Wednesday as Democrats and Republicans appeared to be coming together in a challenge of President Barack Obama’s oversight of the project. In a series of rapid developments that unfolded just hours after Congress returned from a seven-week recess, there were indications the measure could pass and be sent to Obama in the coming weeks.

- This article, from activist Jess Worth, discusses how she was monitored by British Petroleum because of her activists activities. She also believes the BP hired out to a security firm to do the same.

- As the week of climate action known as Beyond Extreme Energy came to a close in Washington, D.C. on Friday, activists blockaded the entrance to the Federal Energy Regulatory Commission (FERC) building for the fifth day in a row in a final push to fight the commission’s approval of fracking projects around the country.

- Tribal and environmental groups have sued the U.S. State Department for approving a temporary plan by a Canadian pipeline company to increase the flow of heavy crude oil from Alberta into Minnesota before a federal environmental study is finished. The lawsuit, filed Tuesday in U.S. District Court in Minnesota, alleges that the State Department violated the National Environmental Policy Act and other laws in approving the temporary increase in oil flow and in not releasing information about it. The suit seeks an injunction to halt the project.

- A federal appeals court on Wednesday threw out a Royal Dutch Shell lawsuit that was intended to inoculate the company’s oil-spill plans from challenges by environmentalists. The 9th U.S. Circuit Court of Appeals said Shell’s 2012 lawsuit against numerous environmental groups, including Greenpeace and the Center for Biological Diversity, represented a “novel legal strategy” but violated the U.S. Constitution.

- A Wednesday evening blast and resulting fire at a Blue Racer Midstream natural gas processing station near Caldwell in Noble County in Ohio killed a worker.

- Marcellus fractivist Wendy Lynne Lee posted a letter from Sandra Steingraber, describing the arraignment of several fractivists related to a recent protest in Seneca Lake, NY.

**Agribusiness**

- Seed companies Monsanto and Dow filed suit in U.S. District Court in Honolulu to overturn a voter-approved moratorium on genetically engineered crops in Maui County, Hawaii.

- A dozen farm groups and agribusinesses agreed on a 10 principles for data privacy and security in the emerging field of agricultural Big Data. They include an assurance that technology companies will not use farm data to speculate illegally in commodity markets. Other guidelines say farmers own the information generated on their land, that farmers can retrieve their data from technology companies, that companies will disclose if they share farm data with others, and companies will protect the privacy of the data.

- Monsanto announced an agreement with soft white wheat growers to settle three class-action lawsuits that arose from the discovery that some of its experimental genetically engineered wheat was growing wild in eastern Oregon. The settlement calls for Monsanto to put $2.125 million into a settlement fund to compensate growers in Idaho, Oregon and Washington state who sold soft white wheat from May 30-Nov 30, 2013 and $250,000 to four wheat grower associations.

- Sustainable Pulse reported on the $25 million independent study of GMO’s and
associated pesticide use that is being launched in London. This is reported to be the world’s largest study on GMO safety, seeking to research the safety of GMO’s and pesticides for human health. The study will officially begin in 2015 and will last 2-3 years, with interim results published at regular intervals throughout.

- A new variety of GM potato that has been approved by the USDA. The Center for Food Safety (CFS) issued warnings to consumers as the GM products will not be labeled as such. The potatoes are produced using a new form of genetic engineering called RNA interference (RNAi). Critics argue that the technology is still not fully understand and the potentially harmful effects of that technology are not yet known. A panel of independent scientists organized by the EPA concluded that there were significant uncertainties surrounding the RNAi technology.

- A new report was published by the Rainforest Action Network on November 11, 2014. The report describes continued palm oil operations by various companies in the Leuser Ecosystem region of Indonesia.

- The European Parliament voted to strengthen the ability of member states to opt out of EU authorization of GMO cultivation. Activists continue to seek to tighten the EU’s GMO authorization process.

- The Global GMO Free Coalition (GGFC) has launched a global fundraising effort to raise money towards the study, Factor GMO. The study is nearing its total goal of $25 million. According to the article, the GGFC’s fundraising campaign will run through April 2015.

- On November 13, 2014, it was announced that the palm oil giant IOI Loders Croklaan has pledged zero-deforestation sourcing requirements for its palm oil trading. The announcement in question comes from the organization Forest Heroes, an organization tied to Rainforest Action Network. With this pledge, the article asserts that now 75% of the world's palm oil trading is accounted for with zero-deforestation policies already in place.

- On November 13, 2014, Sustainable Pulse reports that an open letter published by The Times newspaper and delivered to Downing Street warns the UK over the dangers of GMO crop cultivation. The letter was signed by individuals and organizations including Food and Water Watch, the Sierra Club, Organic Consumers Association and others, representing approximately 57 million members and supporters. This comes ahead of the vote to be taken in January by the European Parliament which may allow member states to decide for themselves whether they will allow GMO cultivation.

- Labor contract disputes at West Coast seaports are slowing Minnesota agricultural exports headed for international markets. The labor disputes compound delays already caused by congested rail lines.

- Four workers were killed and one was injured Saturday during a hazardous chemical leak at a suburban Houston industrial plant, DuPont officials said. The chemical, methyl mercaptan, began leaking around 4 a.m. in a unit at the DuPont plant in La Porte, about 20 miles east of Houston. Plant officials said the release was contained by 6 a.m.

- For the second time this year, a group of U.S. Senators is pressing the FDA to strengthen its oversight of antibiotics that are used in food-producing livestock. In a letter sent yesterday to the agency, the senators want FDA officials to collect data on the extent to which these medicines are used by food producers. At issue is growing concern that humans are becoming increasingly resistant to antibiotics that are widely used in food-producing animals.
Insurance/Healthcare

- The US Department of Veterans Affairs released its monthly data incidents report to Congress for October, some of which involved compromised protected health information (PHI). There were a total of 765 veterans affected, 640 of which were in relation to PHI incidents.

- Healthcare privacy and security issues are part of several topics that the Office of the National Coordinator (ONC) plans to focus on over the next decade. The ONC recently released an outline of its new whitepaper describing its 10-year vision for advancing health IT capabilities and work toward an interoperable health IT infrastructure.

- CareAll Management, also known as CareAll Home Services, a Nashville-based home health care provider, will pay $25 million following claims the company overbilled government health care programs and charged for procedures that were not medically necessary.

- Clinical workflows – an established process in a clinician’s daily activity of caring for patients – are increasingly integrating with healthcare information systems, and therefore, healthcare security. The nation’s push to transition hospitals from paper to electronic health records (EHR) has unquestionably introduced long hours of administrative overhead.

- It would be greatly beneficial to patients if healthcare privacy policies were stronger, according to newly adopted policies at the American Medical Association’s (AMA) Interim Meeting. Specifically, health insurance companies need to take greater care to ensure that there is no accidental disclosure of patients’ protected health information (PHI).

- Healthcare data encryption is becoming an increasingly hot topic, especially as more providers implement EHRs and work to develop strong BYOD policies across their organizations. No one wants to make headlines for a healthcare data breach, especially if the cause was easily avoidable. By making sure that data is encrypted when it is stored locally on devices – data at rest – and when it is sent from one device to another – data in motion – healthcare organizations can ensure that patients’ protected health information (PHI) is safe from unauthorized users.

- The Centers for Medicare and Medicaid Services says it has implemented a number of security improvements to the HealthCare.gov website and systems as the agency gears up to launch the second annual open enrollment period for the Affordable Care Act.

- It’s critical to review the requirements of HIPAA technical safeguards to ensure that your healthcare organization is compliant and able to keep PHI safe.

Financial

Financial Services

Activism

- A 48-hour nationwide bank strike took place in Argentina from November 12th to November 13, 2014, impacting some settlement and cash operations.

- An activist group created a petition that demands several leading investment banks “pay reparations to descendants of African slaves.” The petition alleges that a leading U.S. financial firm’s two predecessor banks “had ties to slavery.”
Several anti-capitalism march events took place Tuesday, November 11, 2014 in cities across the U.S., including Seattle, Los Angeles, and NYC.

A protest in solidarity with 12 arrested ‘Flood Wall Street’ protesters from September 22, 2014 will occur at the NYC courthouse on December 8, 2014 from 8:30am to 4:30pm EST. Participants intend to enter the courtroom, and remain on the streets outside the courthouse brandishing their ‘Flood Wall Street’ signage.

A social media post calls to boycott a list of companies, many of which are financial firms, regarding their anti-gun stance.

A social change organization launched an online petition calling for criminal charges against a leading U.S. investment bank regarding the bank’s alleged attempt to pay a whistle blower to keep quiet.

**Information Security Risk**

A hacktivist campaign known as Operation Darknet released a target list of 164 websites, most of which belong to financial institutions and U.S. intelligence agencies, which have some linkage to child pornography. The operation seeks to disrupt the targeted websites, likely via DDoS attacks.

Chinese government hackers are suspected of breaching the computer networks of the United States Postal Service, compromising the data of more than 800,000 employees. The intrusion was discovered in mid-September.

Researchers said for at least four years an espionage campaign dubbed “Darkhotel” has been stealing sensitive data from selected corporate executives travelling abroad. “Darkhotel” hits its targets while they are staying in luxury hotels. Recent targets included top executives from the US and Asia doing business and investing in the APAC region. The Darkhotel actor(s) maintains an effective intrusion set on hotel networks, and tricks victims into downloading and installing a backdoor that pretends to be an update for legitimate software - Google Toolbar, Adobe Flash or Windows Messenger.

A leading global security firm claims the Russian Government is actively “condoning” hacks on Western retail and banking businesses.

A leading home improvement chain that recently suffered a security breach said hackers stole about 53 million email addresses in addition to customer data for 56 million payment cards previously disclosed by the retailer.

A prominent hacktivist collective doxed a leading U.S. post-trade financial firm, exposing extensive and critical employee and IT infrastructure data in the open source.

The Turkish unit of a leading UK investment bank was compromised by hackers and lost 2.7 million customers’ bank account data. The breach is limited to Turkey. An investigation is underway, no attack details have been disclosed.

A hacktivist collective attacked the website of a leading investment bank in Mexico on November 14th, rendering the site inoperable for an undisclosed time period.

A hacktivist collective claimed on November 14, 2014 to have stolen nearly 1,500 Israeli credit cards.

**Legal, Litigation, Regulatory Risk**

In an effort to put an end to taxpayer bailouts of banks considered “too big to fail,” the chairman of the Financial Stability Board and Bank of England governor proposed new bank rules on November 10, 2014 that will have the creditors “pick up the bill when big lenders collapse.” The chairman said in a statement, once implemented, these agreements will play important roles in enabling globally systemic banks to be resolved (wound down) without recourse to public subsidy and without disruption to the wider
An article reported that banks and retailers may be gearing up for a battle over whose responsibility it is to foot the bill when cyber-criminals attack. Industry bodies that represent banks are urging lawmakers to introduce legislation during the new session of Congress next year that would make retailers pay for cleanup costs themselves. Banks argue however that they are picking up the tab for breaches caused by lapses in merchant security protocols.

A leading U.S. Comptroller of Currency figurehead announced at a banker’s conference in Chicago, IL on November 7, 2014 that U.S. community banks and vendors providing services to them should expect more stringent exams to ensure that they have adequate defenses against computer hackers. The purpose of the exams are to reduce the level of systemic risk to the financial industry.

US legislators will table a congressional bill to monitor human rights and political development in Hong Kong, describing the city’s freedoms as “under threat” from Beijing. The Congressional-Executive Commission on China announced the Hong Kong Human Rights and Democracy Act on November 13, 2014, arguing that Washington must back calls for genuine universal suffrage in the chief executive election in 2017. The bipartisan bill would ensure that the United States can continue to monitor Hong Kong while ensuring that its democracy and freedoms remain a cornerstone of US policy.

**Operational Risk**

- A social media post claimed two Senators drafted a plan to “phase out” the two GSEs for housing.
- An activist organization held a workshop, open to the public, on November 14th in Philadelphia, PA to discuss student debt as a political creation to repress youth rebellion, and how it disproportionately affects children of color and working class youth.
- A new grassroots group has surpassed its crowd funding goal of $10,000 to help subsidize costs for travelers to attend its first national convening in Florida on November 13-16, 2014. The group's mission is to train, support, and network grassroots groups to help build a broad and powerful movement for social, political, economic, and ecological justice. The collective states that it prioritizes groups that use direct action to fight for real wins. The purpose of the first national convening is to lay ground for a powerful network of front-line groups ready to rise to the challenge of future movements.
- An environmental activist group finalized its annual direct action manual, and a separate environmental activist group held a promotional fundraiser event in Chicago, IL on November 13, 2014 to promote and distribute the manual. The direct action manual is over 300 pages of diagrams, step by step descriptions of techniques and a comprehensive overview of the role direct action plays in resistance—from planning an action, doing a body blockade, putting up a tree sit or executing a lockdown; to legal and prisoner support, direct action trainings, fun political pranks, and more.
- A likely Occupy Wall Street member took to social media to comment that leading financial firms employ their own intelligence analysts to spy on activities.

**Reputational Risk**

- Theorists believe a leading US post-trade financial services company is involved in an edit war on a popular online encyclopedia source to “cover up lies” about its involvement in naked short selling activities. The accusers state that the post-trade firm and its contributions to naked short selling are similar to the actions of “organized crime.”
- A post made to a popular online computer hardware magazine claimed that a leading
U.S. teachers’ pension fund management company lost half of their savings this year due to "bad investments."

Global Intelligence

China

- Chinese news outlets reported that an employee strike at an Amazon distribution facility affected the facility's normal delivery operations. The strike began around Nov 4, mainly due to dissatisfaction with a new salary assessment scheme which began November 1, 2014. With orders on the decline in recent days, the recalculation method would result in lower pay for employees.

- China Labour Bulletin reported that a group of 56 shoe factory workers in Guangzhou yesterday urged the Guangdong Provincial Federation of Trade Unions to intervene after 7 of their representatives were detained by police for allegedly sabotaging production and business practices. The federation claimed it could not represent workers in their on-going dispute with Xinsheng over compensation terms related to the closure of the factory due to the tough stance taken by management.

- A Chinese technology website reports that Google's mail service was recently hacked, possibly compromising millions of Gmail accounts. Login credentials can not only be used to access Gmail accounts but also third-party sites that use the same credentials. The article provides steps to encrypting user data to protect against future attacks.

- A Chinese technology news outlet reports a hacker hacked into Jiangsu Public Security Vehicle system, deleted more than 14,000 traffic violation and profited more than 6,000,000 RMB.

- A Chinese website reports a security vulnerability on iOS called "Masque Attacks". The attacker could exploit this vulnerability through text messages, email and URL to lure iPhone and iPad users to install malicious applications and disguise as existing application to obtains users’ banking information, mailbox login credentials and other information.

- A Chinese news outlet reports a hackers group dubbed as "Darkhotel" targeting hotel's Wi-Fi network in order to steal information from high level corporate executives who are on business trips overseas. According to the news article 90% of these virus infection cases are in Japan, Taiwan, China, Russia and South Korea.

- A Chinese website reports the pro-Palestinian hacker organization "AnonGhost" successfully breached United Nation website to protest against Israel invasion of Al-Aqsa Mosque in East Jerusalem.

- A Chinese news outlet reports the encrypted chat application on Android contains an unknown-key-share vulnerabilities.

- A Chinese website reports 360 Security came across a malicious Trojan disguised as flashlight application for mobile devices.

- A Chinese security news outlet reports a malware targeting Android devices caught on November 11, 2014, hence dubbed as "Double-11 SMS Thief". The malicious Trojan are able to disguise as an application associated with China Mobile and lure users to download. Once installed, the malwares are able to intercept text message contains online bill pay information and banking information.

- A Chinese technology news outlet reports Android Lollipop contains a high risk security vulnerability that could be exploited to send out any broadcast.

- A Chinese news outlet reports Blizzard World of Warcraft's server experience a DDoS
attacks.

**Korea**

- Business Korea reported that 19 workers and bereaved family members of workers who contracted incurable diseases such as leukemia during their service in electronic companies filed for industrial accident compensation on October 28, 2014. The civic organization of Banolim, which represents semiconductor manufacturing workers, held a press conference and received their application forms that day in front of the Korea Workers' Compensation and Welfare Service building located in Seoul. The 19 applicants are divided into nine from Samsung Semiconductor, three from Samsung LCD, two from Samsung Electro-Mechanics, one from the IT and Mobile Division of Samsung Electronics, two from LG Display, one from Seoul Semiconductor, and one from SK Hynix. A total of 62 such applications have been filed via the organization since June 2007.

**Malaysia**

- A human right activist Charles Hector posted a blog posting suggesting companies' directors and owners should be liable for money owe to the workers if the companies suffer financial difficulties.

- MTUC shared a news article on its blog regarding MTUC claimed that Malayan Railwayare guilty of union-busting activities and confirmed that the company terminated 41 and suspended 45 union members.

- A Malaysian news outlet reports the human resources minister states that foreign workers could control Malaysian economy due to its large population.

**North America**

- Medical Press reported that nearly a quarter (23%) of US respondent indicated they have been diagnosed with depression in their lifetime and two in five (nearly 40%) of those patients reported taking time off work - an average of 10 days a year - as a result of their diagnosis.

**United Kingdom**

- Tech Crunch reported that Amazon is expanding its R&D operations in Cambridge, U.K., with a plan to staff out a large research lab — expanding on the foothold it acquired when it bought Cambridge-based speech tech start-up Evi Technologies two years ago.

**Vietnam**

- Vietnam Breaking News reported that a draft law pending in the Department of Occupational Safety under the Minister of Labor, Invalids and Social Affairs may require employers to pay 1% of insurance premium for the occupational accident insurance for contract laborers.

- Vietnam Breaking News reported that the VNese government has issued a new decree to increase the minimum wage by 250,000 VND - 400,000 VND ($11.8-$18.9 USD)/month starting January 1, 2015 for laborers in all four of the country's wage zones.

**Legal and Regulations**

- In an effort to push retailers to adopt heightened security for credit and debit cards, President Barack Obama signed an executive order mandating chip-and-PIN technology for government cards. While the order applies only to government-issued
cards and card terminals, the President took the opportunity to urge all stakeholders to “drive the economy towards more secure standards to safeguard consumer finances and reduce their chances of becoming victims of identity theft – America’s fastest growing crime.”

- Recent weeks have seen a flurry of legislative activity in California in the privacy space. On September 29, 2014 Governor Jerry Brown signed into law two bills regarding student privacy. On September 30, 2014 he signed into law eight bills addressing privacy concerns related to invasion of privacy, distribution of unauthorized images, and data collection and security.

- At the end of October, the National Institute of Standards and Technology (NIST) released its draft Guide to Cyber Threat Information Sharing. This document is intended to provide guidance on improving the efficiency and effectiveness of defensive cyber operations and incident response activities through the improvement of information sharing. Additionally, the draft guide also looks at how to improve the planning, implementation and maintenance of information sharing programs. NIST plans to issue a final guidance document sometime next year. Comments are due on the draft guidance by Friday, November 28, 2014.

- Last week, a White house official, speaking anonymously, confirmed there had been a cyber-attack on the Executive Office of the President network. A second US official said there were no indications that the White House’s classified networks, which are kept separate from day-to-day traffic, had been affected. As a result of the attack, White House officials were asked to change their passwords and users faced temporary outages.

**Worldwide**

- In a world-first, the Australian Government has announced it will makes 100 years of intellectual property (IP) rights data available online, to make finding collaboration partners easier and allow the mapping of innovation. The information being made available comprises more than 350 million data points, including rights to patents, trade-marks, designs and plant breeders’ rights and will be updated annually.

- Canada’s new “notice and notice” regime for Internet copyright infringement will come into effect on January 2, 2015. The regime provides a mechanism for copyright owners to give notice of Internet-related copyright infringement claims to Internet intermediaries, who are required to respond to a notice in a specified manner or face liability. The Canadian notice and notice regime is significantly different from the “notice and take down” regime established by the United States Digital Millennium Copyright Act, which requires an Internet intermediary who receives notice of alleged infringing material to expeditiously remove or disable access to the material or face possible liability for copyright infringement. Under the Canadian regime, Internet service providers and Internet storage service providers are not required to remove or disable infringing content, although they may do so voluntarily, and a copyright owner will still be required to invoke other legal remedies (e.g. commencing copyright infringement proceedings) against the infringer. Internet intermediaries should now be preparing to comply with the notice and notice regime, including: (a) implementing policies and procedures for processing infringement notices, forwarding infringement notices to alleged infringers, retaining relevant records for the prescribed period (for Internet service providers and Internet storage service providers) and deleting unauthorized reproductions (cached copies) of works (for Internet search engine providers); and (b) making appropriate amendments to their customer agreements and terms of use.

- China’s Supreme People’s Court recently issued a judicial interpretation regarding breaches of personal rights on the internet. The interpretation detailed the legal liabilities that arise in a data breach case, including who was liable. The interpretation has been hailed as a step forward in terms of litigating a breach case but businesses are urged to take note of the potential increases in exposures in relation to data protection compliance.
Pharmaceuticals

- FDA commissioner Margaret Hamburg will push Chinese officials to grant visas for inspectors in a visit to China this week, part of an effort to make sure food and medicine made abroad is safe for Americans.

- Doctors are testing seniors for drugs such as heroin, cocaine and “angel dust” at soaring rates, and Medicare is paying the bill, writes The Wall Street Journal, noting this is a roundabout result of the war on addiction to prescription painkillers.

- A Spanish provincial court has released details of a five-month-long police investigation into allegations that one of the country’s leading pharmaceutical distributors has been illegally exporting state-subsidized medicines.

- The United States Department of Justice Antitrust Division (DOJ) recently served two U.S.-based generic pharmaceutical manufacturers with criminal grand jury subpoenas. It is reported that the subpoenas request all communications discussing generic pharmaceutical pricing and sales with competitors, and that they are not limited to particular products. The subpoenas signal a much broader federal investigation into potential Sherman Act violations in the generic pharmaceutical industry—with potential criminal implications for the companies and individuals involved. It is unusual that the DOJ, and not the Federal Trade Commission’s Bureau of Competition (FTC), is investigating this industry and certainly significant that the DOJ issued criminal grand jury subpoenas to do so.

- Vascular Solutions Inc. and CEO Howard Root were indicted on eight counts of selling an unapproved medical device and one count of conspiracy Thursday. Federal prosecutors in San Antonio, Texas, said the Maple Grove-based medical device company marketed its Veri-Lase Short Kit varicose vein-treatment device for uses not approved by the Food and Drug Administration.

Retail

- Market Watch reported that Dollar General is partnering with St. Jude’s Children’s Research Hospital’s Thanks and Giving campaign and the U.S. Marine Corps Reserve Toys for Tots Foundation’s “You’re the Hero” toy drive, as well as other local toy drives, to offer customers an opportunity to give back this holiday season. More than 11,500 Dollar General stores will collect gifts to benefit the Toys for Tots until December 8, 2014. In addition, Dollar General will donate $100,000 to Toys for Tots.

- CNN Money reported that Big Lots has created a new national occasion to serve as the basis of a promotion. The leading closeout retailer has declared November 16-22, 2014 as the nation’s first “Decorate Your Home for the Holidays Week,” to provide inspiration and motivation to shoppers to begin decking the halls this holiday season.

- Best Buy and Sports Authority joins the list of stores that will be open on Thanksgiving Day. Target said deals will be available on Target.com Thanksgiving morning and then stores will open at 6 p.m. that evening.

- The Des Moines Register reported that Dahl's Foods Inc., the 83-year-old Des Moines-based grocery store chain, filed a $41 million bankruptcy petition in federal court Sunday asking that it be allowed to reorganize and sell its stores. The likely buyer will be its supplier or another grocery company.

- Reuters reported that a group of Walmart employees pushing for higher wages said on Friday they were planning protests at 1,600 Walmart stores nationwide on Black
Friday. The labor group, Our Walmart, said it had protested 1,200 to 1,400 Walmart stores last year on Black Friday, the day after the Thanksgiving holiday.

- A lockout or strike at West Coast ports would take $1.9 billion of GDP out of the American economy on a daily basis, according to Macy's Inc. CEO Terry Lundgren.

- House Speaker John Boehner doesn’t plan to move a bill along that would allow states to require e-tailers to collect sales tax.

- Alibaba Group Holding Ltd. says consumers purchased $9.3 billion worth of goods during the annual 24-hour sales event that takes places each year on November 11th in China. For the first time, Alibaba extended the promotion beyond China and says consumers in 217 countries purchased on Alibaba e-commerce sites during the sale.

- Increasingly worried about the state of their cyber security, and unable to hire or retain specialist staff, U.K. firms are looking to hire hackers and ex-convicts in a desperate bid to secure their networks.

- Germany’s foreign intelligence agency plans to spend millions to penetrate the secure connection technologies used by social networks, banks and online shops.

- Burger King’s server has been hacked By AnonGhost, including all of its country domains.

Technology

- Symantec reports that a campaign was launched called, Operation CloudyOmega targets Japan’s Ichitaro product line. The blog post highlights that the exploit is sent to targeted organization via a malicious Ichitaro document file attached and that payloads from the exploit may include several backdoors aimed to steal confidential information from the compromised system.

- Masque Attack can be used to replace legitimate iOS apps, such as banking of social networking apps were installed through Apple’s official App Store. The Masque Attack is used by the WireLurker malware which allowed unapproved apps designed to steal information downloaded from the Internet.

- A North Little Rock man is in jail after police said he was caught stealing AT&T phone lines for copper. According to Lt. Carl Minden, Forrest Wayne Collier, 48, of North Little Rock, is accused of stealing copper from AT&T telephone wires in the Blue Hill area. He was booked into the Pulaski County Jail for five counts of theft of property, one count of theft by receiving, and one count of failure to appear. Figures from police records suggested that Collier made over $22,500 in damage to AT&T property and took around 2,506 feet—that's almost half a mile—in phone lines.

- A collective of large tech companies has urged the Senate to pass the USA FREEDOM Act, a bill that it could vote on this week. Reform Government Surveillance, which counts Google, Apple, Microsoft, and Twitter as members, released a letter to the Senate, calling the week’s vote an “opportunity” to pass the “bipartisan” law. The Act will, according to the companies, prevent “bulk collection of Internet metadata,” and increase “transparency about government demands for user information from technology companies.”

- The Wall Street Journal published a report claiming that the U.S. Justice Department is “snagging [mobile data belonging to] a large number of innocent Americans” via technology that can identify criminal suspects using planes. The WSJ cites sources who claim that the U.S. Marshals Service is using fake cell towers on airplanes — dubbed ‘dirtboxes’ — in order to access data from phones located on the ground.
Telecommunications

- Net Neutrality advocates blockaded the driveway of FCC Chairman Tom Wheeler in protest of the FCC’s anticipated ruling on the matter. The advocates claim that Mr. Wheeler is not representing the public and that he is working for companies like Verizon and AT&T, as the protesters cite Wheeler’s prior experience to FCC as a lobbyist for cable and telephone corporations.

- According to CEO, Randall Stephenson, AT&T is halting the rollout of its gigabit fiber Internet service, which launched in Austin, Texas last year. The delay is expected to last until there are solid net neutrality rules in place to follow.

- The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) published guidelines for IT penetration testing and website checks, outlining procedures and requirements for efficient and effective pen testing. The guidelines can also be used to identify appropriate external vendors – e.g. vendors certified by the BSI – and to define the scope of work. While the guidelines describe the general setting of pen testing and explain technical terms, they do not provide details of the testing itself. The guidelines are meant for businesses and government agencies.

Entertainment

- Brooklyn Nets fans trying to locate the team’s schedule or recent score may have typed “nets.com” into their browser and been redirected to a variety of sites unrelated to the team. The Nets do not own the domain Nets.com and the rightful owner has been playing tricks on the team’s fans with their antics.

Defense

- A Chinese hacker going with the handle of "M4ix#4s" from "1937 CN Team" has hacked and defaced the official website of Federal Transit Administration (FTA) of U.S. Department of Transportation. Hacker left a deface note along with a message in Mandarin Chinese language. The reason for targeting U.S. Department of Transportation website wasn’t mentioned anywhere.

- Chinese APT1, also known as "Comment Crew" has been "persistently targeting China-focused rights groups as well as International rights groups."

- Chinese hacker group believed to be associated with the Chinese government has penetrated the Australian media organizations. Sources reports that APTs "Deep Panda" and "Vixen Panda" are targeting Australian media organizations in an attempt to "understand the domestic media climate when Chinese president Xi Jinping arrives."

- Chinese hackers have been implicated in the United States weather system hack in October 2014, disrupting satellite feeds and other high-profile websites.

- The State Department has taken the unprecedented step of shutting down its entire unclassified email system as technicians repair possible damage from a suspected hacker attack. A senior department official said Sunday that activity of concern was detected in the system around the same time as a previously reported incident that
targeted the White House computer network. That incident was made public in late
October, but there was no indication then that the State Department had been
affected.

- The US arm of BAE Systems filed a lawsuit on 12 November to protect itself from a
USD43 million penalty after South Korea's Defense Acquisition Program
Administration (DAPA) cancelled a USD1.7 billion contract to upgrade 134 Republic of
Korea Air Force F-16 combat aircraft.

- Federal employees and contractors scattered across more than a dozen agencies,
from the Defense and Education departments to the National Weather Service, are
responsible for at least half of federal cyberincidents each year since 2010, according
to an Associated Press analysis of records.

---

**Law Enforcement**

- From Boston to Los Angeles, police departments are bracing for large demonstrations
when a grand jury decides whether to indict a white police officer who killed an unarmed
black teenager in Ferguson, Missouri. The St. Louis County grand jury, which has been
meeting since Aug. 20, 2014 is expected to decide this month whether Officer Darren
Wilson is charged with a crime for killing Michael Brown after ordering the 18-year-old
and a friend to stop walking in the street on August 9, 2014. The shooting has led to
tension with police and a string of unruly protests there and brought worldwide attention
to the formerly obscure St. Louis suburb, where more than half the population is black
and yet few police officers are.

- North Dakota’s oil boom has brought with it an upswing in crime. To combat the rising
crime, the FBI is opening a permanent office in northwest North Dakota, the Associated
Press reports. The crime is fed by a population increase and has included human and
drug homicides and organized crime. Although the FBI has offices in Bismarck, Grand
Forks, Fargo and Minot, they are still a long drive to the northwest part of the state.

- The Justice Department has been collecting data from cell phone users on a mass scale
for the past seven years by using electronic devices to mimic cellular towers, the Wall
Street Journal reports. The U.S. Marshals Service reportedly flew Cessna planes with
technology capable of simulating cell phone towers. The planes have flown out of at least
five metropolitan airports but have a “flying range covering most of the U.S. population.”
By collecting data this way, the Justice Department doesn’t have to get records from cell
phone companies.

- Widespread corruption, misconduct and abusive behavior were found in Alabama’s prison
system following a six-month investigation by a nonprofit law firm. Now the firm, the
Montgomery-based Equal Justice Initiative, is urging the Justice Department to conduct a
formal investigation, the Montgomery Advertiser reports. Alleging extreme violence,
security problems and a culture of fear at the prisons, the firm filed a lawsuit against the
Alabama Department of Corrections last month.

- Federal drug enforcement agents showed up unannounced Sunday to check at least
three visiting NFL teams' medical staffs as part of an investigation into former players’
claims that teams mishandled prescription drugs.

- There were no arrests, Drug Enforcement Administration spokesman Rusty Payne said
Sunday. The San Francisco 49ers' staff was checked at MetLife Stadium in East
Rutherford, New Jersey, after they played the New York Giants. The Tampa Bay
Buccaneers' staff was checked at Baltimore-Washington International airport after playing
the Redskins. The Seattle Seahawks, who played at Kansas City, confirmed via the
team's Twitter account that they were spot-checked as well. The spot checks were done
by investigators from the federal DEA. They did not target specific teams, but were done
to measure whether visiting NFL clubs were generally in compliance with federal law.
Agents requested documentation from visiting teams' medical staffs for any controlled substances in their possession, and for proof that doctors could practice medicine in the home team's state.

- Los Angeles police are increasingly relying on technology that not only tells patrol officers where crime is most likely to occur but also identifies and keeps track of ex-cons and other bad guys they believe are most likely to commit them. Police say the effort has already helped reduce crime in one of the city's most notorious and historically gang-ridden neighborhoods. Dubbed LASER for its ability to zero in on offenders and hotspots, it is one of many newer law enforcement tools that use data tracking and collection — such as license plate scanners and cellphone trackers — often with little public knowledge or regulation. Privacy advocates say LASER isn't transparent, has no clear oversight and unjustly focuses on keeping ex-convicts under suspicion even though they've served their time.