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

Beyond Buzzwords: Defining Threat Intelligence and Why It Matters:

In this webcast, the first in a two-part series, we'll look at what defines threat intelligence, and why not knowing what it is can cost your organization and hurt your security posture.

What you’ll learn in this webcast:

• What characterizes true threat intelligence
• Why what you don’t know about threat intelligence could cost you
• How to evaluate threat intelligence solutions

Top Incidents

Energy

WestCoastNativeNews.com has posted this article reporting that First Nations activists are turning their attention to TransCanada Corp.’s proposed Energy East project, vowing to mount the same kind of public opposition that threatens the Keystone XL pipeline in the United States and Enbridge Inc.’s Northern Gateway in British Columbia. The article adds that some 70 First Nations leaders met in Winnipeg recently to plan a strategy they hope will block TransCanada’s ambitious plan to ship more than 1 million barrels a day of crude from Western Canada to refineries and export terminals in the East, despite widespread political support for the $12-billion project.
Agribusiness

- Twitter post from May 23, 2014, Anonymous claims to have hacked 1800 accounts from Monsanto, Bayer, Dow, Dupont, Syngenta, “and many others.” There is no explicit mention of Cargill. The tweet has been retweeted 11 times so far. The tweet includes a video originally posted on Vimeo on May 22, 2014. The Vimeo link has been included as a supplemental link.

Insurance/Healthcare

- As part of President Barack Obama’s new final rule that will regulate Affordable Care Act (ACA) standards for patient protection, the Centers for Medicare & Medicaid Services (CMS) and Department of Health and Human Services (HHS) will be looking to hand out civil money penalties when data privacy and security issues arise out of the health insurance exchanges.

Financial Services

- The world’s largest online auction company based in San Jose, CA issued a statement asking its customers to “change their passwords because of a cyberattack that compromised a database containing encrypted passwords and other non-financial data.”

Global Intelligence

- The US Department of Justice indicted five officers of the Chinese People’s Liberation Army for allegedly hacking into networks of several US companies. In response, Beijing denounced the charges and later announced plans for tighter checks on Internet technology companies that do business in China.

Energy

- BP is asking the U.S. Supreme Court to hear its challenge of the settlement agreement that’s forcing the oil company to reimburse businesses deemed hurt by the massive 2010 Deepwater Horizon spill in the Gulf of Mexico. BP said Monday that it wants the Supreme Court to review its claim that the settlement process is rife with fraud. The company argues that it’s been ordered to pay “hundreds of millions of dollars – soon likely to be billions – of fictitious and inflated losses.”

- The Guardian discusses how the previous conception of US shale deposits is overestimated. The article notes that next month, the US Energy Information Administration (EIA) will publish a new estimate of US shale deposits set to deal a death-blow to industry hype. EIA officials told the Los Angeles Times that previous estimates of recoverable oil in the Monterey shale reserves in California of about 15.4 billion barrels were vastly overstated. The revised estimate, they said, will slash this amount by 96% to a puny 600 million barrels of oil.

- The Huffingtonpost.com assesses the safety of coastal nuclear plants in the US with regards to rising sea levels cause by the effects of climate change.

- WestCoastNativeNews.com has posted this article reporting that First Nations activists are turning their attention to TransCanada Corp.’s proposed Energy East project, vowing to mount the same kind of public opposition that threatens the Keystone XL pipeline in the United States and Enbridge Inc.’s Northern Gateway in British Columbia. The article adds that some 70 First Nations leaders met in Winnipeg recently to plan a strategy they hope will block TransCanada’s ambitious plan to ship more than 1 million barrels a day of crude from Western Canada to refineries and export terminals in the East, despite widespread political support for the $12-billion project.
The Obama administration is investigating the health risks of hydraulic fracturing after at least four deaths among oilfield workers since 2010 in North Dakota and Montana. The National Institute for Occupational Safety and Health said the workers were exposed to high levels of volatile hydrocarbons during the drilling process known as fracking. The institute is asking oil and gas drillers to help assess the risks of exposure to chemicals in used fracking fluids. It is recommending that companies develop different ways to measure the fluid stored in tanks and to provide hazard awareness training.

Washington state’s newest Rising Tide chapter, Rising Tide Bellingham, recently held an anti-oil train protest, where they symbolically blocked train tracks. This action was considered symbolic because the protesters dispersed before actually causing a disruption to train traffic. This appears to be the group’s first protest.

A new report by the Sierra Club and Earthjustice is critical of the number and condition of coal ash ponds in the United States. The report calls for new environmental regulations governing coal ash ponds.

Activists in Massachusetts, who are on trial for conducting a lobster boat blockade to obstruct delivery of 40,000 tons of coal to the Brayton Point power plant, are attempting to employ a “necessity defense” to justify their actions.

The Department of Justice announced Monday charges against five Chinese military hackers, accusing them of stealing trade secrets and other proprietary or sensitive information online. The hackers targeted big-name makers of nuclear and solar technology, stealing confidential business information, sensitive trade secrets and internal communications for competitive advantage, according to a grand jury indictment. The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity. “This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking,”

Everglades Earth First! announces that the Chesapeake Earth First! is hosting an Energy Exports Action Camp June 2-9 in Prince George’s County, Maryland.

Peaceful Uprising will host the California Student Sustainability Coalition (CSSC) from July 15-22, 2014 to build relationships with activists and organizers throughout the Western region, and learn about direct action resistance, all while cultivating and consistently honoring an analysis based in climate justice principles.

A public utility in the U.S. was compromised after attackers took advantage of a weak password security system, according to a U.S. Department of Homeland Security team that studies cyberattacks against critical infrastructure. The utility’s control system was accessible via Internet-facing hosts and used a simple password system, wrote the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in a report on incidents covering the first quarter of this year. The utility, which was not identified, was vulnerable to a brute-force attack, where hackers try different combinations of passwords until the right one is found. An investigation showed the utility was attacked before. “It was determined that the systems were likely exposed to numerous security threats, and previous intrusion activity was also identified,” ICS-CERT wrote in the report.
• @OpGreenRights is claiming plans of an operation against the European Union. There may be more after the MAM is over.

• The Rainforest Action Network has begun a new campaign to target the Kuala Lumpur Kepong Berhad (KLK), one of the largest suppliers of palm oil. RAN published a paper decrying the company’s environmental abuses in April. This campaign is focusing on their operations in Papua New Guinea.

• Twitter post from May 23, 2014, Anonymous claims to have hacked 1800 accounts from Monsanto, Bayer, Dow, Dupont, Syngenta, “and many others.” There is no explicit mention of Cargill. The tweet has been retweeted 11 times so far. The tweet includes a video originally posted on Vimeo on May 22, 2014. The Vimeo link has been included as a supplemental link.

### Insurance

• The Government Accountability Office has confirmed it will conduct “complete and continuous end-to-end testing” of the security of the Obamacare HealthCare.gov website and systems.

• Employee benefits broker Maschino, Hudelson & Associates (MHA) recently began notifying approximately 5,500 employees of its customers that their personal information may have been exposed when a laptop was stolen from the trunk of an MHA employee’s car on or about April 2, 2014.

• In cooperation with the Los Angeles Police Department, the National Insurance Crime Bureau has produced new high definition videos showing some of the most common methods of staging motor vehicle accidents to defraud insurance companies.

• Healthcare organizations and their business associates should take a number of crucial steps to prepare for potential breach investigations and HIPAA compliance audits by the Department of Health and Human Services.

• As part of President Barack Obama’s new final rule that will regulate Affordable Care Act (ACA) standards for patient protection, the Centers for Medicare & Medicaid Services (CMS) and Department of Health and Human Services (HHS) will be looking to hand out civil money penalties when data privacy and security issues arise out of the health insurance exchanges.

• Approximately 1,800 students’ personal information may have been captured by keylogging malware on computers at the University of California Irvine (UC Irvine) student health center, which were infected for a six-week period.

• As more and more employees are using their personal devices, such as smartphones and tablets, for work purposes, having a mobile security plan in place becomes paramount.

• A Senate bill widening avenues of fraud data-sharing will better enable private and public health insurers to jointly disrupt crooked medical providers from looting both sectors, enabling insurers and law enforcement to freely exchange case and trend data without being vulnerable to defamation suits by persons being discussed during confidential case reviews.

• Canada’s Eastern Health recently announced that one of its employees had inappropriately accessed 20 patient records. All affected patients are being notified, and the employee in question has resigned.
• At least several dozen, but possibly hundreds, of confidential medical records were scattered to the winds outside Research Hospital on Monday afternoon, potentially exposing the personal and medical information of scores of former patients of Midwest Women’s Healthcare.

• Idaho’s Larsen Dental Care recently announced that an undisclosed number of patients’ personal and medical information may have been exposed when an unencrypted external hard drive was stolen from an employee’s vehicle on March 4, 2014.

• Blue Cross and Blue Shield of Kansas City (Blue KC) recently began notifying 2,546 of its members that a former employee may have stolen their financial information. The breach, which was discovered on February 26, 2014, was limited to those members who had spoken with the employee in question regarding payment of their premiums.

• The Federal Trade Commission recently said it would crack down on the sharing of information about children by mobile apps, and there are now indications that it will turn its regulatory gaze toward apps that collect health data.

Financial Activism

• Housing activists held a bank auction “teach-in” in Santa Ana, CA on May 20th, condemning “city lawyers, clerks, and government employees” for not doing enough to stop California homes from being lost to foreclosure.

• An activist group launched a petition against a leading U.S. bank for its alleged “$3 billion tax break” and collected over 150,000 signatures. The group plans to deliver the petition to Attorney General, Eric Holder.

• A Northern Virginia-based religious group challenged a leading U.S. bank at its shareholders’ meeting held last week in Tampa, FL to invest at least $60 million in equity to “rebuild neighborhoods.”

• Housing activists held a protest against “foreclosures, evictions, and utility shutoffs” at Detroit Water Department Office in Detroit, MI on May 23rd.

• Activists launched a petition against a leading U.S. investment bank, demanding the firm divest from food companies involved in the “cruel treatment of pigs.”

• A U.S.-based environmental activist group launched a petition against a leading French investment bank, demanding the bank divest from funding coal mining companies involved in the mountaintop removal practices.

• A UK activist group will protest against a European telecommunications company in Central London on June 14th for being a perceived tax-dodger and “stealing billions of pounds of public money.”

• Housing activists will hold a protest at Tim Geithner’s book singing event in Santa Clara, CA on May 29th for his “failed policies that only works for Wall Street while Main Street continues to suffer.”

• Activists held a protest outside a leading U.S. investment bank in New York City on May 19th, demanding the firm not attend the Saint-Petersburg International Economic Forum scheduled for May 22nd in Russia and end cooperation with Vladimir Putin’s regime.
An anti-GMO march was to take place throughout the Financial District in San Francisco, CA on May 24th. Participants were slated to organize at Union Square and march to Howard and 3rd Street for a short press conference, then proceed down Howard to UN Plaza for a speak-out on issues surrounding GMO chemical agriculture.

Occupy activists breached the facility entrance of an investment bank in Ireland on May 22nd and protested within. The purpose of the occupation was to bring awareness to continued bank bailouts.

Environmental activists protested at a leading European investment bank's shareholders meeting in London on May 23rd, demanding the bank "pull out of coal" and stop fueling climate change.

**Information Security Risk**

- A hacker group claimed to have hacked over 60 American websites.
- A hacker group allegedly uncovered a SQLi vulnerability in the main server of a leading U.S. bank, granting access to an entire database of credit cards.
- A new study released by a leading U.S. network security firm found that 97% of the networks experienced some form of breach, despite the use of multiple layers of network and computer security software. The study analyzed data from more than 1,600 networks over a six-month period from October 2013 to March 2014. On average, each network was subjected to 1.6 exploits and 122 malware droppers during the six-month period. In addition, 27% of the monitored organizations in the study "experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors," inferring that they were being attacked by either state-sponsored organizations or sophisticated criminal networks.
- Researchers say criminal hacker groups are zeroing in on Silverlight vulnerabilities in order to spread malware that leads to system compromise and data loss for victims.
- Researchers say the software in most home routers is so "obsolete and riddled with known vulnerabilities" that it is an inviting attack surface for hackers. The researchers also said using rigorous passwords and encryption will help a little, but not all that much.
- Researchers say infections of porn site-related ransomware known as "Kovter" have more than doubled over the past month to top 15,000 times. Kovter typically targets users of adult websites, taking control of the computer or mobile device. It then pops-up a message claiming the user has broken the law and must pay a fine by a certain time to avoid prison time. If no adult site browsing history can be found the malware creates that evidence by redirecting the victim's browser to an adult site before logging and retrieving content.
- Researchers recommend that Adobe Shockwave should be uninstalled because not only does the software require constant updating, and also few sites actually require the browser plugin, it bundles a component of Adobe Flash that is more than 15 months behind on security updates, and which can be used to backdoor virtually any computer running it.
- Threat researchers are urging organizations with a stake in south-east Asia to invest in advanced cyber intelligence to counter a growing number of Chinese espionage operations against entities in the Philippines, Vietnam and elsewhere in the South China Sea (SCS).
- Security researchers say Russian cybercrime gangs are currently using the iBanking Android Trojan that is touted to be of commercial quality and one of the most expensive...
pieces of malware seen on the underground market. Subscriptions to the software, including tech support, are being sold for almost £3,000 (US $5,000). The malware relies on social engineering to lure victims to download the program onto their devices and is used to intercept one-time banking passwords sent through SMS, or to construct mobile botnets and conduct covert surveillance on victims. The Trojan can be configured to look like official software from a range of different banks and social networks.

- Researchers warn that a new version of a notorious piece of malware known as MiniDuke has been identified. The malware is an extremely small and highly customizable, assembler-based backdoor that was used in the past to target mostly government entities and institutions around the world. The exploit used to deliver the malware is that of the recently patched Word RTF Memory Corruption Vulnerability (CVE-2014-1761) and comes in the form of a specially crafted RTF file named Proposal-Cover-Sheet-English.rtf, delivered via email.

- Researchers say a new exploit kit known as Infinity is being offered on underground markets for $100 per day. The Infinity kit takes advantage of vulnerabilities in Firefox, Internet Explorer and Opera – as well as flaws in plug-ins, such as Adobe Flash – to compromise browsers and upload malware.

- Internet security researchers say a critical security flaw in Microsoft’s Internet Explorer 8 has gone unfixed since October 2013. The vulnerability allows an attacker to run malicious code in IE 8 when you visit a website designed to infect your computer.

- The United States Computer Emergency Readiness Team announced that Cisco has released two security advisories to address multiple product vulnerabilities, one of which may allow a remote attacker to execute arbitrary code with elevated privileges.

- The world’s largest online auction company based in San Jose, CA issued a statement asking its customers to “change their passwords because of a cyber-attack that compromised a database containing encrypted passwords and other non-financial data.”

- A group of hackers from the Netherlands and Morocco claimed to have compromised the security of Apple’s iCloud system for locking iOS devices. The hack will unlock stolen iPhones by bypassing Activation Lock, making it possible for thieves to resell the phones easily on the black market. It also may provide hackers with access to Apple ID passwords and other personal information stored in Apple’s iCloud service.

- As many as half a million payment cards have been compromised by ‘Nemanja,’ a recently discovered piece of malware that has infected nearly 1,500 point-of-sale (POS) devices. The massive, worldwide Nemanja botnet, discovered in March by a cyber-intelligence company, includes more than 1,478 hosts in more than 35 countries across the world, including the U.S., UK, Canada, Australia, China, Japan, Israel and Italy, as well as other developing countries. Reportedly, the botnet is the work of a single group of cyber crooks believed to be located in Serbia, and that the U.S., namely New York, California, Washington and Colorado, have been high priority targets.

- A security firm issued a threat advisory warning on May 22nd regarding a spike in DDoS attacks abusing the Simple Network Management Protocol (SNMP) interface in network devices such as routers, switches, firewalls, and printers. The firm spotted 14 SNMP DDoS attack campaigns over the past month, targeting various industries including consumer products, gaming, hosting, nonprofits, and software-as-a-service, mainly in the US (49.9%) and China (18.49%). The attackers used a tool that’s available online and was developed by the infamous hacker group Team Poison.

Legal, Litigation, Regulatory Risk

- The head of the Financial Industry Regulatory Authority, Inc. (FINRA) said high-frequency trading firms should be required to register with U.S. securities
regulators. The self-regulatory organization said it is cracking down on abusive high-frequency trades and currently has some 170 ongoing investigations on the subject.

- Three U.S. public companies identified as Chinese hacking victims didn’t report the theft of trade secrets and other data to investors, despite rules designed to disclose significant events. Two of the companies said the thefts weren’t “material” to their businesses and therefore don’t have to be disclosed under SEC rules designed to give investors information that may affect share prices.

- An article claimed that even weeks after the deadline for the start of the new EMIR regulation requiring companies to report all derivative trades to new European trade repositories, many firms are still believed to be non-compliant. Some believe the new system could take up to a year to bed down.

- A tech industry group that has Facebook, Google, Yahoo, AOL, Apple, Microsoft, Twitter and LinkedIn as participants rejected President Obama’s support May 21st for the swift passage of the USA Freedom Act by the U.S. House of Representatives, and urged the Senate to follow suit. The Act aims to put curbs on surveillance by the National Security Agency. The tech industry group, called Reform Government Surveillance, says the latest draft opens up an “unacceptable loophole that could enable the bulk collection of Internet users’ data.”

**Operational Risk**

- Student activists in southern Florida pressed their school’s foundation this month to heed a 10,000 person-strong petition and divest from U.S. investment firms linked to Israeli occupation.

- American financial services corporations are considering pulling out of Russia because a new law there would require them to pay steep fees to continue operating in the country.

**Reputational Risk**

- A Washington, D.C.-based non-profit organization claimed that Iranian students across the United States are “having their financial lifeline severed, often with little or no warning, by one of the largest banks in the United States.”

- An article published on a career website last week claimed more big banks are hosting their annual meetings outside their home states to avoid picket lines and verbal assaults from shareholders and retail customers, and, that “their plans are working incredibly well” as shareholders have asked minimal, if any, opposing questions during the meetings.

- The U.S. Securities and Exchange Commission is investigating two American investment firms over whether they are doing enough to police their clients’ identities, noting that the regulator is looking into whether the brokerages missed red flags that could indicate attempts to move money illicitly or to feed proceeds from illegal activities into the financial system.

- Activists claimed that banks are starting to force borrowers into agreeing to “gag orders” as a condition for granting mortgage modifications under HAMP, an action they state is “coercive and unethical” and possibly illegal. The gag orders are allegedly included in mortgage modification paperwork, and state that the borrower cannot say or print or post anything negative about the provider.
· Housing activists held a bank auction “teach-in” in Santa Ana, CA on May 20th, condemning “city lawyers, clerks, and government employees” for not doing enough to stop California homes from being lost to foreclosure.

· An activist group launched a petition against a leading U.S. bank for its alleged “$3 billion tax break” and collected over 150,000 signatures. The group plans to deliver the petition to Attorney General, Eric Holder.

· A Northern Virginia-based religious group challenged a leading U.S. bank at its shareholders’ meeting held last week in Tampa, FL to invest at least $60 million in equity to “rebuild neighborhoods.”

· Housing activists held a protest against “foreclosures, evictions, and utility shutoffs” at Detroit Water Department Office in Detroit, MI on May 23rd.

· Activists launched a petition against a leading U.S. investment bank, demanding the firm divest from food companies involved in the “cruel treatment of pigs.”

· A U.S.-based environmental activist group launched a petition against a leading French investment bank, demanding the bank divest from funding coal mining companies involved in the mountaintop removal practices.

· A UK activist group will protest against a European telecommunications company in Central London on June 14th for being a perceived tax-dodger and “stealing billions of pounds of public money.”

· Housing activists will hold a protest at Tim Geithner’s book singing event in Santa Clara, CA on May 29th for his “failed policies that only works for Wall Street while Main Street continues to suffer.”

· Activists held a protest outside a leading U.S. investment bank in New York City on May 19th, demanding the firm not attend the Saint-Petersburg International Economic Forum scheduled for May 22nd in Russia and end cooperation with Vladimir Putin’s regime.

· An anti-GMO march was to take place throughout the Financial District in San Francisco, CA on May 24th. Participants were slated to organize at Union Square and march to Howard and 3rd Street for a short press conference, then proceed down Howard to UN Plaza for a speak-out on issues surrounding GMO chemical agriculture.

· Occupy activists breached the facility entrance of an investment bank in Ireland on May 22nd and protested within. The purpose of the occupation was to bring awareness to continued bank
Environmental activists protested at a leading European investment bank’s shareholders meeting in London on May 23rd, demanding the bank “pull out of coal” and stop fueling climate change.

Global Intelligence

China

- A Chinese technology news outlet reports information regarding iBanking, an android malware that has been called the Swiss Army Knife of malware due to its multiple capabilities. According to the article iBanking could infect PC and mobile devices, disguised itself as normal application, intercept banking SMS, and access location data and file system. It also able to be controlled remotely, and connect infected devices to Botnet. Its anti-analytic skill allowed it to not work properly in a virtual machine, in order to prevent cracking or counterfeiting.

- A Chinese news outlet reports two Bitcoin trading platform suspended withdrawal due to hacker attacks.

- A Chinese news outlet reports collaboration of police forces of 19 countries arrested a group named Blackshadel, which specialize in creating, utilize and sell malwares.

- Filipino hackers reportedly attacked almost 200 Chinese government and private websites in retaliation against China for their aggressive actions in the (West Philippine Sea (South China Sea) The hacking campaign has been dubbed “OpChinaReloaded”.

- The US Department of Justice indicted five officers of the Chinese People’s Liberation Army for allegedly hacking into networks of several US companies. In response, Beijing denounced the charges and later announced plans for tighter checks on Internet technology companies that do business in China.

- The China Labour Bulletin reported that according to a new survey by the National Bureau of Statistics, published May 12th, per capita living expenses in China have increased by 21.7 percent on average in 2013 to reach 892 yuan per month. In comparison, monthly wages for China’s rural migrant workers have only increased 13.9 percent over the last year. The report figures seem to indicate that low pay is still a major problem in China and will continue to be a factor in labor disputes for the foreseeable future. Although the focus of many recent factory strikes has been compensation for lay-offs, relocation and change of ownership etc., low pay is often cited by workers as their most pressing grievance.

- Digitimes reported that despite Taiwan-based companies becoming targets last week in anti-China protests, the Taiwan-based makers will continue to expand business in Vietnam, as labor costs in the country are significantly lower than in China, sources said.

- Chinese news outlets reported that over 1000 workers at Japan-based KONICA MINOLTA factory in Dalian went on strike against unfair severance compensation. Police reportedly intervened to maintain control.

- Digitimes reported that six ex-Foxconn Electronics employees, who were being investigated by prosecutors in Taiwan starting January 21, 2014, have been officially indicted for asking for bribes from upstream suppliers.
Germany

- Parties generally seen as skeptical towards the idea of European integration were successful in elections for the EU parliament. In France, the right-wing Front National won more than a quarter of all votes and became the strongest party in this election. In the UK, the United Kingdom Independence Party (Ukip), hostile towards the very idea of European integration, was the first party other than Labour and Conservatives to win an election in over a century. In Italy, a coalition of populist movement Five Stars and xenophobe Lega Nord reached over 30 per cent (yet were not the strongest party). Among the biggest EU member states, only Germany somewhat buckled this trend. The Alternative for Germany (AfD) won seven per cent. The political outfall remains to be seen, e.g. whether or not more established parties will try to slow down the process of integration.

Ireland

- The Irish Central reported that the police in Ireland have won the right to organize themselves as a legal trade union and go on strike for the first time.

Korea

- Arirang News reported that according to the International Trade Union Confederation gave South Korea the worst possible ranking of level 5 in it Global Rights Index. A level 5 means there is “no guarantee of rights” in the country.

North America

- Montgomery County, Maryland—a suburb of Washington, DC—has lured an enterprise security startup from neighboring Virginia after making the county’s first financial investment in a cybersecurity company. The $100,000 funneled to Mobile System 7 from Montgomery County’s economic development fund represents the first deal in an investment strategy that will likely become more aggressive in the coming years. The investment comes as economic development officials plan to host the first Cyber Montgomery Forum Thursday, bringing together leaders from the public and private sectors to discuss the cybersecurity’s potential impact on the region. Mobile System 7 collected $1 million from investors last month with funds run by the State of Maryland and Montgomery County kicking in a combined $400,000.

- Forbes reported that HP will lay off more people than it initially planned. According to the article, an additional 11,000 to 16,000 positions will be eliminated from the company’s workforce.

- CNN Money reported that Amazon will be using 10,000 robots in its warehouses by the end of the year. There are currently 1,000 robot workers on the Amazon floors. According to the article, the increase won’t change the number of actual people employed.

- Times Union reported GlobalFoundries $10 billion expansion of it’s Fab 8 is happening so rapidly that the company is going to use as many as 200 workers from IBM to help complete the project. According to the media source, GlobalFoundries has 2,200 employees at Fab 8, as well as 600 contractors working to help the plant with the expansion of its 300,000 square-foot clean room.

- Minds reported Samsung just released a public apology for the dangerous chemicals workers in their factories were exposed to, causing 56 documented cases of leukemia.

- Threat Post reported that a new information sharing and analysis center (ISAC) has been formed to support the retail industry. The Retail Cyber Intelligence Sharing Center, known as R-CISC, includes an ISAC as well as training and research components. The
organization comprises a number of prominent retailers, including Safeway, Nike, Gap, Lowe’s and Target.

**Malaysia**

- On 5/21/2014, a Malaysian human right activist, Charles Hector posted a blog posting disapproves the MMA (Malaysian Medical Association) president statement on Medical Certificate (MC). He states that it is absurd employers has the right to decide the medical state of employees and choose whether to accept the Medical Certificate (MC) or not.

- On May 18, 2014, a Malaysian news outlet reports MTUC apposed to the Good and Services Tax implementation in April of next year and urging the government to abandon the proposal. MTUC claims that the tax will further burden the low and medium income groups.

- A Malaysian news outlet reports pig DNA found in Cadbury products and several non-government organization urging Cadbury Confectionary Malaysia to stop all operation and recall all their product.

**Vietnam**

- Yahoo! News reported that Foxconn let workers in its Vietnam facilities take three days off for safety reasons.

- Yahoo! News reported that Chinese business in Vietnam have suspended production in Vietnam in response to the rioting that occurred in Vietnam.

- Yahoo! News reported that Vietnam flooded major cities with police to avert anti-China protests on 5/18/2014 while Beijing evacuated thousands of citizens after a flare-up over disputed sovereignty in the South China sea sparked rioting in Vietnam last week.

- Dan Tri News reported that the Chairman of Vietnam General Confederation of Labour, Vietnam’s only official union, called on workers to protest against China in a proper manner.