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

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

Top Incidents

**Energy**
- 44 Greenpeace activists were arrested in Rotterdam as they attempted to stop a Russian tanker from unloading its shipment of Arctic oil.

**Agribusiness**
- On May 5-6, 2014, the Forest Asia Summit, Jakarta, will bring together CEOs, Southeast Asian ministers, civil society leaders and development experts and scientists to discuss a move towards a greener economy. They hope to bring about
commitments to improving the environmental impact of economies as well as commitments to sustainable investments and policy options.

**Insurance/Healthcare**

- According to the results of a recent survey of 4,880 global IT security professionals, 57 percent of respondents don’t think their organization is protected from advanced cyber-attacks, and 63 percent don’t think they can prevent the exfiltration of confidential information.

**Financial Services**

- The United States Computer Emergency Readiness Team, a part of Homeland Security known as US-CERT, said in an advisory released on April 28th that computer users should consider using alternatives to Microsoft’s Internet Explorer browser until the company fixes a security flaw that hackers have used to launch attacks. Researchers warn that a sophisticated group of hackers have been exploiting the bug in a campaign dubbed “Operation Clandestine Fox,” targeting U.S.-based firms, currently tied to defense and financial sectors.

**Global Intelligence**

- In attempt to address a deficiency of skilled cybersecurity professionals, global IT association ISACA has launched a new initiative called Cybersecurity Nexus (CSX). CSX has been developed in collaboration with chief information security officers and cybersecurity experts from leading global enterprises and government agencies. It seeks to provide a central location where security professionals can find cybersecurity research, guidance, certifications, education, mentoring and community. A recent study by Cisco estimates that close to 1,000,000 positions for security professionals remain unfilled. Another report by the World Economic Forum/McKinsey estimates that if unresolved, these challenges could cost the global economy $3 trillion.

**Legal and Regulations**

- Proposed amendments to the Delaware General Corporation Law (DGCL) are being considered by the Corporation Law Section of the Delaware State Bar Association. If approved by the Corporation Law Section and the Executive Committee of the Delaware State Bar Association, the proposed amendments will be considered by the Delaware legislature. The effective date for the proposed amendments would be August 1, 2014.

**Energy**

- The American Bird Conservancy is suing the federal government for issuing 30-year kill permits to wind farms. The U.S. Fish and Wildlife Service originally wanted to grant five-year permit but the wind industry complained that five years was not enough time to find financial backers and get the project up and running. The US FWS will now issue 30-year permits which must be reviewed every five years. Michael Hutchins, the American Bird Conservancy’s bird-smart wind energy coordinator claims the 30-year permit will make the process less transparent, “data on things like bird fatalities at a particular institution might be hidden from us, and therefore, it would be very difficult to do a legitimate review of what is exactly going on at any one of those facilities.”

- Oklahoma Attorney General Scott Pruitt and Oklahoma Gas and Electric, the state’s largest utility, haven’t had much luck going up against the U.S. Environmental Protection Agency lately. As StateImpact has reported, Pruitt and OG&E are still waiting to hear whether the U.S. Supreme Court will hear their challenge to the EPA’s regional haze rule, after lower courts sided with the
agency’s attempt to clear the air on federal lands. But if Tuesday’s ruling is any indication, the Supreme Court doesn’t appear sympathetic to Pruitt’s concerns about federal overreach. In a 6-2 decision, the court on Tuesday revived the EPA’s cross-state pollution rule, which is separate from the regional haze rule, but would also require coal-fired power plants to reduce emissions. The issue now goes back to a lower court for more consideration.

- 44 Greenpeace activists were arrested in Rotterdam as they attempted to stop a Russian tanker from unloading its shipment of Arctic oil.

- The American Lung Association released its annual "State of the Air" report today, and its disturbing overall finding was: "Nearly half of all Americans - more than 147 million - live in counties in the U.S. where ozone or particle pollution levels make the air unhealthy to breathe." The long-standing problem of smog throughout the country is another why it's so important that we continue to move beyond coal to clean energy. Pollution from coal-fired power plants leads to smog (or ground-level ozone), a toxic compound and a dangerous irritant. Doctors liken inhaling smog to getting a sunburn on your lungs. It can cause chest pain, coughing, and breathing difficulties. It triggers asthma attacks, and it can lead to irreversible lung damage or even death. Smog exacerbates conditions like bronchitis, emphysema, and asthma - sometimes fatally.

- Article reports that a new study from the National Research Council is warning that neither the science nor the currently available public or private response infrastructure is anywhere near prepared for an oil spill in the Arctic Ocean. The findings, funded by multiple federal agencies as well as the oil and gas industry, offer a potent new obstacle to attempts to drill in the Arctic, particularly as the study’s publication follows a string of related setbacks. Environmentalists say the new research validates warnings they have been voicing for years.

- Oil Free Otago have slammed New Zealand Petroleum and Minerals (NZPAM) for skipping crucial democratic steps in consulting with the public over oil and gas exploration, and labelled the event “a PR Stunt". Last night, New Zealand Petroleum and Minerals held a meeting at Araiteuru Marae to explain and answer questions on aspects of the Government's regulatory regime for petroleum and minerals exploration and production. This meeting pre-empt the vital stages before it; asking and correctly educating the Dunedin community what type of energy expansion options and economic opportunities there are in our neighbourhood. Oil Free Otago demands this base-assumption; that oil and gas is the only exploration option, is put under the spotlight. “At no point were Dunedinites asked if this is the direction that we want to see our energy development to go” asks Oil Free Otago spokesperson Danielle Triford. “Rather than asking the initial, primary and basic questions to help shape energy expansion paths, Dunedinites were only allowed to hear about the already set-in-place regulations for exploration and production of oil and gas.”

**Agribusiness**

- Activist group Rainforest Action Network (RAN) has set a goal to collect 60,600 photo petitions – one per each orangutan remaining in the wild – to deliver to the ‘Snack Food 20’, the top snack food companies that are alleged to use conflict palm oil.

- On May 5-6, 2014, the Forest Asia Summit, Jakarta, will bring together CEOS, Southeast Asian ministers, civil society leaders and development experts and scientists to discuss a move towards a greener economy. They hope to bring
about commitments to improving the environmental impact of economies as well as commitments to sustainable investments and policy options.

- On May 1, 2014, TFT announced on their website that Johnson and Johnson has become their newest member. TFT is a global NGO working with companies to improve their sustainability policies.

- On April 30, 2014, an article by Sustainable Business Consultant, Robert Hii, was published about upcoming legislation in Indonesia regarding rainforest protection. A large agriculture company is mentioned when the author quotes their recent No-deforestation policy, and points out possible loopholes or parts of the policy that would be dependent on government protection of rainforest.

---

**Insurance**

- DDoS attacks on Boston Children's Hospital's website have security experts debating whether these attacks could become far more common in healthcare.

- Faced with a vulnerability that exposes Microsoft's Internet Explorer Web browser to a zero-day exploit involved in recent targeted attacks, CISOs need to take prompt action, security specialists say. That includes communicating the vulnerability to end users, using alternate Web browsers, and developing an incident management strategy.

- Willis North America recently began notifying an undisclosed number of employees that their personal information may have been exposed when a health plan administrator mistakenly attached a spreadsheet containing sensitive data to an e-mail sent on March 19, 2014, to company employees who were enrolled in the Willis North America Medical Expense Benefit Plan's Healthy Rewards Program.

- The Pocono Record reports that a laptop that may have held the personal and medical information of 733 Coordinated Health patients was stolen from an employee's car in Bethlehem, Pa., on February 21, 2014. The laptop, which was password-protected but doesn't appear to have been encrypted, hasn't been recovered.

- A White House working group exploring big data and privacy has proposed that Congress enact a national data breach notification law as well as legislation to define the government's role in cybersecurity.

- One of the biggest misunderstandings about the Heartbleed bug in the healthcare sector is that it only affects websites and Web servers. In fact, medical devices are also at risk for the vulnerability.

- The Baltimore Sun reports that the Social Security numbers of 2,166 former Johns Hopkins University students were mistakenly made available online. According to university spokesman Dennis O’Shea, the university discovered on March 19, 2014 that the names and Social Security numbers of 2,166 people who had studied at the university's Homewood campus between 2007 and 2009 had been stored on a publicly accessible server.

- Amedisys Inc. and its affiliates have agreed to pay $150 million to the federal government to resolve allegations that they violated the False Claims Act by submitting false home health care billings to the Medicare program. Amedisys, a Louisiana-based for-profit company, is one of the nation’s largest providers of home health services and operates in 37 states, the District of Columbia, and Puerto Rico.

- Mercy Regional Medical Center Mercy employees, according to the Durango Herald,
were the target of a phishing email attack in which the hackers tried to obtain user names and passwords. Some employees, under the impression it was an authentic email, responded and provided their system login information. Exactly what entity, perhaps Centura, the hackers were posing as is unknown at this point.

- A breach involving the posting of information about 15,000 Boston Medical Center patients on a transcription firm's unsecured website serves as a reminder of the importance of monitoring the security practices of all business associates. Boston Medical Center was notified on March 4 by another healthcare provider that MDF Transcription Services and its subcontractors "had incorrectly posted BMC physician office visit notes to the MDF website without password protection," a Boston Medical Center spokeswoman tells Information Security Media Group.

- DeKalb Health hospital announced on Wednesday that it had learned of a hacking incident involving the DeKalb Health website that resulted in inappropriate access to certain information about some DeKalb Health patients. DeKalb Health uses a third party firm to operate its website, and a computer server operated by that third party was the target of an overseas hacking attack that potentially impacted three different groups of DeKalb Health patients.

- Texas Attorney General Greg Abbott's office has reached a $10 million agreement with West-Ward Pharmaceuticals Corp. to settle allegations that the New Jersey company committed Medicaid fraud by inflating prices.

- DataBreaches.net reports that a former Snelling Staffing employee recently exposed 9,757 people's personal information, including their names, birthdates, home addresses, driver's license numbers, Social Security numbers, medical information, drug tests results, and any alleged criminal activity.

- According to the results of a recent survey of 4,880 global IT security professionals, 57 percent of respondents don't think their organization is protected from advanced cyber-attacks, and 63 percent don't think they can prevent the exfiltration of confidential information.

- Tufts Health Plan recently announced that the names, birthdates, and Social Security numbers of approximately 8,830 current and former members of Tufts Medicare Preferred had been stolen.

- A new study from Neustar shows DDoS attacks in the United Kingdom are often used as a smoke screen for malware attacks or theft. Of organizations surveyed that had a breach tied to a DDoS attack, 53 percent said the installation or activation of malware was involved, while 42 percent stated the assaults masked the loss of funds, customer data, or intellectual property.

- A new voluntary privacy and security certification program for covered entities in Texas aims to bolster compliance with HIPAA and state regulations - and perhaps help organizations avoid federal sanctions. The Texas Health Services Authority developed the new Texas Covered Entity Privacy and Security Certification in partnership with the Health Information Trust Alliance, or HITRUST.

- Reading Health System has put hundreds of patients on notice about the disappearance of their medical billing records. In a letter sent Tuesday to patients of the former Western Berks Internal Medicine, the health system's chief compliance officer, Kathleen Wetzel, said that three boxes of medical billing records, from Jan. 2, 2009 through June 3, 2010, were taken from the practice, apparently in March 2012, and returned on March 24, 2014.
Financial

Activism

- Housing activists protested outside a leading U.S. bank branch in Irvington, NJ on April 28th, condemning the bank for foreclosing on homes.

- Housing activists launched a petition against a leading U.S. bank in support of a California resident whose house is being foreclosed by the bank.

- Environmental activists launched a petition against multiple financial firms involved in funding mountaintop removal (MTR) operations by coal mining companies.

- Activists launched a divestment campaign targeting a leading U.S. investment firm that has investments in an international defense electronics company engaged in a wide range of programs throughout the world.

- Activists held a protest on May 1st against a leading U.S. bank at Hope Plaza in Los Angeles, California, accusing the bank of corruption.

- Housing activists in San Francisco held a rally on April 30th to stop the eviction of five families from their homes on Ellis Street where they have lived for 12 years, demanding that their landlord withdraw their eviction notices immediately.

- Los Angeles area activists held an anti-foreclosure protest outside a leading U.S. bank branch on Olympic Blvd in downtown Los Angeles, California on May 1st.

- Alleged members of the Anonymous movement published a video calling on citizens from across the world to join them in a global protest. The hacktivists urged people to refrain from using the services of banks and from shopping.

- Activists will hold a protest at the shareholders' meeting of a leading U.S. bank in Charlotte, NC on May 7th, demanding the bank divest from the GMO industry.

Information Security Risk

- The Anonymous hacktivist collective warned they will soon publish a "new, big SQL" from an unidentified bank.

- The Anonymous hacktivist collective alleged it published 27 million credit cards to a data dump site.

- A hacker group alleged it leaked more than 30,000 American credit cards in observance of an operation dubbed, #TheWeekOfHorror.

- Trading on the New Zealand Stock Exchange was delayed 15 minutes on April 27th due to an "unspecified issue."

- Researchers say an organized crime group has launched a “major offensive” against U.S. companies that have international components. The attacks are aimed at extracting money from the companies via wire transfers, and have a high success rate. The attacks employ a combination of social-engineering (both email and phone), compromising trusted partners/third parties, and spoofing email addresses in order to accomplish their goals.

- The United States Computer Emergency Readiness Team, a part of Homeland Security known as US-CERT, said in an advisory released on April 28th that computer users should consider using alternatives to Microsoft’s Internet Explorer browser until the company fixes a security flaw that hackers have used to launch attacks. Researchers
warn that a sophisticated group of hackers have been exploiting the bug in a campaign
dubbed "Operation Clandestine Fox," targeting U.S.-based firms, currently tied to
defense and financial sectors.

- U.S. officials and security specialists are warning that Russian hackers may respond to
  new sanctions by attacking the computer networks of U.S. banks and other companies.
  Security researchers claim Russian hackers are believed to have already infiltrated U.S.
  computer networks, and if they decide to retaliate for new sanctions on its banks and
  Putin associates, it could be difficult to trace any cyber-attacks to his government
  because hackers can easily mask their identities and locations online.

- Nine members of a London-based gang have been convicted and three others are
  scheduled for sentencing in June for a series of electronic bank robberies. Using social
  engineering to install a remote-controlled keyboard-video-mouse (KVM) switch on bank
  PCs, the gang managed to transfer millions to outside accounts in two separate jobs in
  April and July of 2013. They were caught attempting to rob a third bank in September.

- A leading U.S. online services company urged all its customers last week to change
  passwords and security questions, as it determined that information for at least two
  percent of all its accounts had been compromised. That's an impact of half a million
  users.

- A new SMS Trojan with worm-like spreading capabilities has been identified, primarily
  targeting Russian Android users to date. Dubbed “Samsapo,” the malware can also
  extract information (phone numbers, text messages) from the infected device and send it
  to a remote server, can download additional malicious files from predefined URLs, and
  can block phone calls and change alarm settings.

- Researchers say known malware family TSPY_USTEAL has resurfaced. This
  information stealing malware now includes new routines including malicious packers,
  obfuscation, and bundling ransomware.

- A malware infection which drew headlines in January has returned and is using new
  techniques to infect and spread amongst users. Known as Sefnit, the botnet infection
  was spotted in September of 2013 and triggered alarms earlier this year when
  researchers warned that millions of systems were likely infected with the malware.
  Associated with click fraud and bitcoin mining activities, Sefnit was noted for its use of
  the Tor anonymizing network as a means of avoiding detection. Researchers have
  observed the infection spreading in the wild. Once installed, the malware uses its control
  servers to receive orders or, download additional payloads.

- A Romanian researcher claims that Skype leaves its local database unencrypted and
  puts users' sensitive information at risk. All Skype-to-Skype voice, video, file transfers
  and instant messages are encrypted. The researcher however found that Skype leaves
  the user’s full name, birthday, phone numbers, country, city and even full chat
  conversations unencrypted on the hard drive in a known location without any encryption
  or password.

- A Twitter account that was used by a known threat actor group believed to have been
  involved in launching cyber-attacks against US financial companies last year has
  resurfaced and posted content on April 30th for the first time since October 21, 2013.

- A computer researcher in Singapore identified a major flaw in the popular open-source
  security software, OAuth and OpenID, which are used by many websites and tech titans
  including Google, Facebook, Microsoft, and LinkedIn, among others. The researcher
  claims the serious vulnerability “Covert Redirect” flaw can masquerade as a login popup
  based on an affected site's domain.

- The United States Computer Emergency Readiness Team announced on May 1st that
  Microsoft has released out-of-band updates to address a critical use-after-free
vulnerability in Internet Explorer versions 6 through 11, including IE versions running on Windows XP. US-CERT recommends that users and administrators review Microsoft Security Bulletin MS14-021 and apply the necessary updates as soon as possible.

**Legal, Litigation, Regulatory Risk**

- India’s 76-year-old Madras Stock Exchange will cease to exist from May 30 after it failed to adhere to several new regulatory requirements, including increased net worth as outlined by markets regulator Sebi. The shutdown appears imminent unless there is a dramatic change in rules over the next couple of weeks.

- The FBI announced that the agency will introduce a system later this year intended to share information among private businesses about digital intrusions in near-real time. Called “Malware Investigator,” its purpose will be to gather and share intelligence from public, private, and government sources to stop threats before they become problems, mainly by passing information directly from machines to machines.

- On May 2nd the SEC charged a leading New York based stock exchange with failure to comply with their own exchange rules. The exchange’s affiliated routing broker was also named in the SEC’s order. Without confirming or denying the charges, the exchange and its broker agreed to pay a $4.5 million fine to settle the SEC’s claims. According to the SEC’s charges, the exchange and affiliate “repeatedly engaged in business practices that either violated exchange rules or required a rule when the exchanges had none in effect.” Violations occurred between 2008 and 2012.

**Operational Risk**

- A bank-worker advocacy group announced on their social media site it will deliver a petition with worker signatures during a shareholders’ meeting of an unnamed bank in the future.

- A collective of politically radical coders plans to release the first version of Dark Wallet: a bitcoin application designed to protect its users’ identities far more strongly than the partial privacy protections bitcoin offers in its current form. If the program works as promised, it could neuter impending bitcoin regulations that seek to tie individuals’ identities to bitcoin ownership. By encrypting and mixing together its users’ payments, Dark Wallet seeks to enable practically untraceable flows of money online that add new fuel to the Web’s burgeoning black markets.

- A major European marketplace organizer and transaction services provider will let members opt out of a block-trading partnership established with buyside-only trading venue Liquidnet last year, following concerns from brokers that the service could reveal sensitive trade information to the rest of the market.

- Police officers were called to the headquarters of a major British bank in London's Canary Wharf at 9:00am on the morning of Thursday, May 1st and conducted a controlled explosion on a suspicious package. The threat was a false alarm and the investigation is now closed.

**Reputational Risk**

- An op-ed that appeared on a website that has 9.7 million members across 16 countries commented on bankers in other countries being harshly punished and executed for “their crimes” and calls for harsher measures against U.S. bankers.

- A new study says one-third of consumers stop shopping at retailers that have been breached, and nearly one-third ditch their healthcare providers after they’ve been breached.

- An activist group launched a petition targeting a leading U.S. bank for its alleged push for a ‘cashless society.’ According to the petition, the bank banned the use of cash for
direct deposits into customer bank accounts under the guise of preventing money laundering and the misuse of customer accounts.

- An activist group launched a petition against a leading U.S. bank, demanding that the bank stop discrimination against adult film industry workers.

Global Intelligence

China

- A Chinese news outlet reports the National Computer Virus Emergency Response Center of China found a new trojan malware that able to rename executable file after it copy itself to specific folder of infected operating system. According to the article, the malware is able to release a malicious dynamically linked DLL component, shut down the security services function, and forcing the operating system to access specified active malicious URL.

- Digitimes reported that Foxconn Electronics and Hewlett-Packard will establish a joint venture for the purpose of manufacturing servers for cloud computing and offering related supporting services. While the partnership went into effect May 1st, Foxconn did not reveal details about the joint venture.

Germany

- Email accounts associated with the state government of Hessia (Hessen), Germany have been compromised in a hacking attack earlier this year. The government responded to a parliamentary inquiry and stated that 50 accounts were identified as compromised. The Hessian authorities followed a tip from authorities in neighboring state Lower Saxony.

India

- Tech 2 reported that Nokia India has informed its employees union that the Chennai plant needs to cut down on staff.

North America

- In attempt to address a deficiency of skilled cybersecurity professionals, global IT association ISACA has launched a new initiative called Cybersecurity Nexus (CSX). CSX has been developed in collaboration with chief information security officers and cybersecurity experts from leading global enterprises and government agencies. It seeks to provide a central location where security professionals can find cybersecurity research, guidance, certifications, education, mentoring and community. A recent study by Cisco estimates that close to 1,000,000 positions for security professionals remain unfilled. Another report by the World Economic Forum/McKinsey estimates that if unresolved, these challenges could cost the global economy $3 trillion.

- The Phoenix Business Journal reported that the AZ economy will add only 53,500 jobs this year according to a new economic analysis from the state Department of Administration.

- IGN reported that Avram Miller, a retired Intel Corp. vice president, says that Apple is working on a Google search engine competitor that will be unveiled in fall 2015.

- Bloomberg reported that a community group and municipal employee union filed a lawsuit against the Google shuttle buses as part of a social justice protest. The defendants in the lawsuit include the city's transit system, Bauer’s Intelligent Transportation Inc., technology companies that use the shuttles and other transit firms.
The defendants are accused of violating a state law that prohibits private buses from parking in bus zones.

- Giga OM reported that Amazon is building a chip design center for its Amazon Web Services cloud business in Austin, TX.

- Business Insider reported that unions in the San Francisco Bay Area are hoping to unionize Apple security guards and hopes that other companies in the region will follow its lead. To that end, the union has protested outside Apple’s store down San Francisco and created a browser-based video game showing how difficult it is to live in Silicon Valley on security officer’s income.

- The AlterNet reported on the class-action lawsuit against Silicon valley tech companies. User called the case one of the largest wage theft cases in American history.

- Forbes reported on the anti-poaching lawsuit against Silicon Valley tech companies. User stated that the employees settled for $325 million, which user considers to be peanuts compared to the allegations of what had been going on. The supplement contains other articles regarding this lawsuit.

Legal and Regulations

- New gTLD UPDATE: As of 4/29/14, the top ten new gTLDs cumulatively hold 45% of all new gTLD registrations. There 249 new gTLDs available. The current leader, .guru (with 53,195), got off to a fast start only to see the momentum quickly fade. New #4, IDN 在线 (Chinese for .online), introduced just yesterday, had an impressive debut in the 30,000 neighborhood.

  - Top 10 new gTLDs:
    - 1) .guru (53,195 registered domains)
    - 2) .berlin (46,914 registered domains)
    - 3) .photography (33,851 registered domains)
    - 4) IDN 在线 (29,719 registered domains)
    - 5) .email (25,973 registered domains)
    - 6) .link (22,973 registered domains)
    - 7) .today (21,890 registered domains)
    - 8) .tips (20,991 registered domains)
    - 9) .company (16,614 registered domains)
    - 10) .technology (14,214 registered domains)

- Proposed amendments to the Delaware General Corporation Law (DGCL) are being considered by the Corporation Law Section of the Delaware State Bar Association. If approved by the Corporation Law Section and the Executive Committee of the Delaware State Bar Association, the proposed amendments will be considered by the Delaware legislature. The effective date for the proposed amendments would be August 1, 2014.

- In a March 20, 2014 letter, the Federal Trade Commission (FTC) offered guidance as to the factors to consider in evaluating whether entry into a contest on a social media site is a form of material connection requiring disclosure under the FTC Endorsement Guidelines. At issue before the FTC was a promotional contest held by Cole Haan on Pinterest. The letter is one of the first instances in which the FTC has offered guidance as to the applicability of the Endorsement Guidelines to contests conducted on social media sites. In light of this new guidance from the FTC, advertisers that incorporate contests on social media platforms like Facebook, Pinterest and Instagram as part of their advertising strategies should pay close attention to the structure of such contests, and especially the nature of any “prize” awarded to the winner, to ensure that such
promotions are legally compliant.

- Kentucky's Governor has signed a bill adding his state to the other 46 states requiring notice in the event of a data breach. Starting in July, companies that hold information about Kentucky residents and who suffer a data breach—defined in that state as an unauthorized acquisition of “unencrypted and unredacted computerized data” that compromises the security of that data or is likely to lead to identity theft—will now be required to notify state residents. Data that triggers the laws' requirements (if breached) is name and social security number, driver's license number, or account number/credit card number in combination with any required security code to permit access to a person's financial account. Section 2 prohibits cloud computing service providers from processing “student data” for any purpose other than providing, improving, developing, or maintaining the integrity of their cloud computing services unless they receive express permission from the student’s parent. H.B. 232 also prohibits cloud computing service providers from using student data in advertising and from selling, disclosing, or otherwise processing student data for any commercial purpose.

- Iowa's Governor has signed an amendment to the state's data breach notification law requiring notice to that state's Attorney General in the event of an incident requiring notice to Iowa residents. The amendment, effective July 1, requires notification to the AG within five business days of notice to affected individuals if the breach affects more than 50 Iowans.