



Homeland
Security

Daily Open Source Infrastructure Report

13 December 2012

Top Stories

- Record fines against National Grid, NStar, and Western Massachusetts Electric Co. (WMECO) were imposed by Massachusetts utility regulators after an investigation by the State into how the utilities planned for and responded to Tropical Storm Irene and a surprise October snowstorm in 2011, the Associated Press reported December 11. – *Associated Press* (See item [1](#))
- Point-of-sale (PoS) systems at major retailers, hotel chains, and restaurants worldwide have been hit by new custom malware that targets the PoS, Dark Reading reported December 11. – *Dark Reading* (See item [5](#))
- Contractors worked through the night to remove and replace an 800-foot swath of Interstate 77 in West Virginia that turned from asphalt to cinder in a massive natural gas line explosion that also flattened four homes and damaged five more but caused no deaths. – *Associated Press* (See item [10](#))
- A suspect killed two people and wounded another before taking his own life December 11 at the Clackamas Town Center southeast of Portland, Oregon. – *Clark County Columbian*; *Associated Press*; *Los Angeles Times* (See item [34](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
 - [National Monuments and Icons](#)
-

Energy Sector

1. *December 11, Associated Press* – (Massachusetts) **Mass. energy regulators fine utilities \$24.8 million for inadequate response to 2011 storms.** Record fines against National Grid, NStar, and Western Massachusetts Electric Co. (WMECO) were imposed by Massachusetts utility regulators after an investigation by the State into how the utilities planned for and responded to Tropical Storm Irene and a surprise October snowstorm in 2011, the Associated Press reported December 11. Hundreds of thousands of customers lost electricity and many waited longer than a week for the lights to come back on after each storm. The largest penalty was assessed against National Grid, which was fined nearly \$8.2 million for Irene and more than \$10.5 million for the snowstorm — a total of \$18.7 million. NStar was fined \$4.1 million — \$2.2 million for Irene and \$1.9 million for the snowstorm. WMECO was fined \$2 million, and only for its response to the snowstorm. The chairwoman of the Department of Public Utilities cited “systematic and fundamental failures in how the company planned for and responded to both storms.” She added, “We also found that many of the problems with National Grid’s response have persisted for some time and the company had been warned about [the problems] in the past,” The investigation also revealed failures in responding to public safety threats posed by toppled electrical wires, she said. National Grid was also cited for lapses in communication with its customers and municipal officials after the storms, and for not prioritizing facilities such as nursing homes while restoring power.

Source: http://www.washingtonpost.com/business/mass-energy-regulators-fine-utilities-248-million-for-inadequate-response-to-2011-storms/2012/12/11/0ce9492e-43b6-11e2-8c8f-fbeb7ccab4e_story.html

For another story, see item [10](#)

[\[Return to top\]](#)

Chemical Industry Sector

Nothing to report

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

See item [23](#)

[\[Return to top\]](#)

Critical Manufacturing Sector

2. *December 11, U.S. Department of Labor* – (National) **OSHA releases online tool to help protect workers exposed to cadmium.** The Occupational Safety and Health Administration (OSHA) December 11 released a new interactive online tool to help protect workers exposed to cadmium. The new interactive online tool will assist employers in complying with OSHA’s cadmium standard. OSHA’s Cadmium Biological Monitoring Advisor analyzes biological monitoring results provided by the user. These data, along with a series of answers to questions generated by the cadmium advisor, are used to determine the biological monitoring and medical surveillance requirements that must be met under the general industry cadmium standard. These requirements include the frequency of additional monitoring and other mandatory components of the employer’s medical surveillance program. The cadmium advisor is primarily intended for use by experienced medical professionals who assess workers’ cadmium exposure. It may also be useful as an educational tool for workers and members of the general public by providing information on what constitutes overexposure to cadmium and what to do to prevent exposure on the job.

Source:

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23391

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Banking and Finance Sector

3. *December 12, Denver Post* – (Colorado) **Feds charge former New Frontier Bank executive with fraud.** A senior executive at the failed New Frontier Bank in Greeley, Colorado, was charged with fraud and money laundering December 11. The man faces

one count each of false bank entries, misapplication, bank fraud, and money laundering. Prosecutors said the man agreed to plead guilty. State regulators shut down New Frontier in April 2009 and appointed the Federal Deposit Insurance Corporation as its receiver. The \$1 billion failure was the costliest bank failure in Colorado history and caused havoc in the agriculture and real-estate communities of northern Colorado. Prosecutors said that from June 2008 to September 2008, after State and federal regulators had directed New Frontier to raise capital, the executive arranged for eight bank customers to borrow money from the bank and use the proceeds to purchase shares of bank stock. That allowed New Frontier to appear to improve its capital position. Prosecutors also alleged that in October 2005 he made false entries into a credit-approval form for a \$5.58 million loan to two borrowers. And that in March 2008, he willfully misapplied \$662,045 of New Frontier's funds, and in June 2008 he deposited \$160,000 into his account to conceal ownership of the money.

Source: http://www.denverpost.com/breakingnews/ci_22169979/officer-defunct-new-frontier-bank-greeley-charged-fraud

4. *December 12, BankInfoSecurity* – (International) **4 banks respond to DDoS threats.** The day after a hacktivist group announced plans to launch a second wave of distributed-denial-of-service (DDoS) attacks on five U.S. banks, SunTrust suffered intermittent outages and Bank of America and PNC said small numbers of their customers reported having trouble accessing their sites, BankInfoSecurity reported December 12. But it remained unclear whether the problems were the result of an attack. PNC used social media to warn consumers that site outages should be expected, but that account and online-banking credentials would remain secure. The online-monitoring site websitedown.com reported that the SunTrust Banks Web site suffered intermittent outages. A Bank of America (BofA) spokesman said that while BofA's site suffered no overall outages, an isolated number of online-banking users reported problems accessing the site. A PNC spokeswoman said some PNC customers may have experienced intermittent difficulty logging in on their first attempts. And a U.S. Bank spokesman said that the bank is "taking all necessary steps" to prepare for more attacks. Source: <http://www.bankinfosecurity.com/4-banks-respond-to-ddos-threats-a-5350/op-1>
5. *December 11, Dark Reading* – (International) **'Dexter' directly attacks point-of-sale systems.** Point-of-sale (PoS) systems at major retailers, hotel chains, and restaurants worldwide have been hit by new custom malware that targets the PoS, Dark Reading reported December 11. Researchers at Seculert, who discovered the so-called "Dexter" malware, did not name names of the companies with the 200- to 300 active attacks against their PoS systems across 40 countries. Most of the victim businesses are English-speaking, with 42 percent based in North America, and 19 percent, in the U.K. The attackers behind the custom-built malware appear to speak fluent English, according to Seculert's chief technology officer (CTO), and do not appear to be the typical Eastern European cybercrime gang. Dexter works by searching the process list in the operating system for PoS software. "It sends out memory dumps to the command and control server, and searches for Track 1 and Track 2 data. These track formats have very unique [markers] so they are easy to find within memory," the CTO said. Some 30 percent of the targeted PoS systems were running Windows Server. Because it is not a

typical OS for browsing, the initial infections were likely via drive by Web downloads or other Web-based attacks. The initial infection vector remains unknown. Dexter also uses an online tool to parse the payment card information, a stealthier approach.

Source: <http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240144190/dexter-directly-attacks-point-of-sale-systems.html>

6. *December 11, Portland Tribune* – (Oregon) **Police catch ‘Hipster Bandit’**. Police arrested the so-called “Hipster Bandit” suspected of a series of bank robberies in Portland, Oregon. The suspect was arrested December 7 after he robbed the Consolidated Community Credit Union. As officers were heading to the credit union, they received additional information that the suspect used a demand note and obtained an undisclosed amount of money. Witnesses provided a detailed description of him to police. Officers converged on the neighborhood near the bank and located a man matching the suspect’s description riding a bicycle away. Detectives identified the suspect, and believe he is responsible for four additional bank robberies in Portland: July 19 at a U.S. Bank branch, August 31 at an Albina Community Bank branch, October 19 at a Key Bank branch, and November 26 at another Key Bank branch.
Source: <http://portlandtribune.com/pt/9-news/124625-police-catch-hipster-bandit>
7. *December 11, WTVF 5 Nashville* – (Tennessee) **Fmr. commissioner admits to \$16M fraud**. A former Robertson County, Tennessee commissioner admitted to operating several Ponzi schemes that defrauded more than 50 local investors out of about \$16 million, WTVF 5 Nashville reported December 11. The former commissioner pleaded guilty to charges of bank fraud, mail and wire fraud, and money laundering. He admitted that his investment schemes, known as the “John Deere Investment,” the “Greenway Investment,” and the “Tennessee in Valley Authority Coal Ash Cleanup Investment,” were fake and that he never intended to invest any of the funds he received from investors.
Source: <http://www.newschannel5.com/story/20319322/fmr-commissioner-admits-to-16m-fraud>
8. *December 11, U.S. Attorney’s Office, District of Connecticut* – (International) **Connecticut federal jury finds Romanian national guilty of participating in Internet phishing scheme**. A federal jury in New Haven, Connecticut, found a Romanian national guilty of conspiracy offenses stemming from his participation in an extensive Internet phishing scheme, according to a court press release December 11. The man was the 10th Romanian citizen convicted as a result of a long-term investigation. Any personal identifying and financial information provided by individuals who fell for the phishing emails would be sent to individuals in Romania or to a “collector” account, which was an email account used to receive and collect the information obtained through phishing. The co-conspirators were part of a loose-knit conspiracy of individuals from Craiova, Romania, and neighboring areas that shared files, tools, and stolen information obtained through phishing. The co-conspirators used and shared a number of collector accounts, which contained thousands of email messages that contained credit or debit card numbers, expiration dates, CVV codes, PIN numbers, and other personal identification information. The co-conspirators then

used the personal and financial information to access bank accounts and lines of credit and to withdraw funds without authorization. The scheme targeted People's Bank, Citibank, Capital One, Bank of America, JPMorgan Chase & Co., Comerica Bank, Regions Bank, LaSalle Bank, U.S. Bank, Wells Fargo & Co., eBay, and PayPal.

Source: <http://www.fbi.gov/newhaven/press-releases/2012/connecticut-federal-jury-finds-romanian-national-guilty-of-participating-in-internet-phishing-scheme>

9. *December 11, KVOA 4 Tuscon* – (Arizona) **Arizona man arrested for fraud after illegal info found on flash drive.** A man was arrested December 7 in Tempe, Arizona, after a tax fraud and identity theft investigation that began early this year when authorities found a flash drive containing hundreds of names and personal information at Cochise College. In February the Sierra Vista Police Department (SVPD) was contacted by Cochise College employees after a flash drive containing 800 to 900 names and associated personal information was left in a school computer. A detective obtained a search warrant for the drive and uncovered files with stolen identities and financial information. Because much of the information involved people from other States, assistance was obtained from the Internal Revenue Service and the U.S. Secret Service. The investigation determined that the man had purchased the names and information online for \$1.50 per name and was using the information to prepare tax returns and place the tax refund money on prepaid debit cards. The names were illegally obtained by Internet phishing scams, a detective from SVPD stated, often via emails made to look like legitimate communications from credit card companies and banks.

Source: <http://www.kvoa.com/news/arizona-man-arrested-for-fraud-after-illegal-info-found-on-flash-drive/>

For more stories, see items [27](#) and [29](#)

[\[Return to top\]](#)

Transportation Sector

10. *December 12, Associated Press* – (West Virginia) **Interstate reopens after W.Va. gas inferno.** Contractors worked through the night to remove and replace an 800-foot swath of Interstate 77 in West Virginia that turned from asphalt to cinder in a massive natural gas line explosion that also flattened four homes and damaged five more but caused no deaths. The December 11 blast between Sissonville and Pocatalico melted guardrails, cooked the green enamel off highway signs and burned utility poles, while leaving a huge hole in the highway. The northbound and southbound lanes reopened December 12. Federal and State agencies were investigating what caused the explosion in the 20-inch transmission line owned by NiSource Inc., parent company of Columbia Gas. The gas flow was shut off, but residents who lived within 1,000 feet of the fire zone were evacuated as a precaution. A NiSource spokesman said the company was still gathering facts and no effects on customers were expected.

Source: <http://abcnews.go.com/US/wireStory/wva-works-reopen-interstate-explosion-17935278#.UMiGJq5JzTo>

11. *December 12, Newark Advocate* – (Ohio) **Granville woman killed in Ohio 37 crash.** Ohio 37 in St. Albans Township, Ohio, was reopened after a crash that left one person dead and sent another to the hospital, the Newark Advocate reported December 12. At the intersection of Moots Run Road and Ohio 37, the driver failed to yield for a stop sign and her vehicle was hit by a tractor trailer traveling north on Ohio 37, according to a release. The road was closed for around 4 hours.
Source: <http://www.newarkadvocate.com/article/20121212/NEWS01/312120028/Crash-closes-Johnstown-Alexandria-Road-injures-two?odyssey=nav|head>
12. *December 11, Associated Press* – (Nevada) **Bad truck brakes blamed for Nevada Amtrak crash.** An inattentive trucker with a history of speeding violations driving a tractor-trailer with faulty brakes was the probable cause of a fatal collision with an Amtrak train that left six people dead in northern Nevada in 2011, the National Transportation Safety Board concluded December 11. The panel also agreed that the weakness of passenger car walls likely contributed to the number of deaths and more than a dozen injuries after the truck skidded 300 feet into the train at a rural crossing on June 24, 2011. It recommended new strength standards be developed. The truck driver was killed along with the train's conductor and four passengers. A NTSB investigator said 11 of the truck's 16 brake drums were worn beyond limits. She said tests conducted by the Nevada Highway Patrol also found 9 of the 16 brakes were out of adjustment or inoperative, but she said the patrol did not use the proper test guidelines so it was not known if those results were entirely accurate. The NTSB found the driver had been cited for 11 speeding violations over the past 10 years but less than half were known to John Davis Trucking Company because the firm only checked his Nevada background. The probe also determined the driver had 30 different employers over the past 10 years but did not include at least 2 that had terminated him on his John Davis application. As a result, the board recommended that commercial motor carriers be required to conduct and document investigations into driver histories for the 10 years prior to their application for employment.
Source: http://www.lompocrecord.com/news/national/ntsb-focuses-on-bad-truck-brakes-in-amtrak-crash/article_b0725685-3907-5053-9373-981852e88684.html

For another story, see item [34](#)

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report

[\[Return to top\]](#)

Agriculture and Food Sector

13. *December 12, Food Safety News* – (Oregon) **Norovirus from Oregon zoo event sickens 90.** The Oregonian reported December 12 that around 90 people fell ill with

gastrointestinal symptoms after attending a meeting of women healthcare professionals at the Oregon Zoo the week of December 3. The meeting was attended by 220 members of the Women's Healthcare Associates group December 5. After the event, nearly 100 people became sick with what officials believe was a Norovirus infection. Health officials are currently looking for the source of the virus, which remained unclear. The most probable scenario is that an infected food worker contaminated food for the catered event that then passed the virus on to other people, a State epidemiologist said.

Source: <http://www.foodsafetynews.com/2012/12/norovirus-at-oregon-zoo-sickens-90/#.UMj30q7kGok>

14. *December 12, Food Safety News* – (International) **FDA renews agreement to collaborate with China on food safety.** The U.S. Food and Drug Administration (FDA) announced December 12 that it renewed an agreement with the General Administration of Quality Supervision, Inspection, and Quarantine of China (AQSIQ) to “enhance cooperation between the U.S. and China on food and feed safety.” The initial agreement was struck in 2007, and the new accord extends the formal cooperation for another 5 years. According to the FDA, the agreement includes enhancement of the FDA’s ability to identify high-risk food products entering the United States from China; collaboration to facilitate inspections of facilities that process and produce food; focus on high-risk foods frequently exported from China to the United States, including canned and acidified foods, pet food, and aquaculture; and the creation of processes for FDA to accept relevant, verified information from AQSIQ regarding registration and certification.

Source: <http://www.foodsafetynews.com/2012/12/fda-renews-agreement-to-collaborate-with-china-on-food-safety/#.UMiiA-TAex8>

15. *December 11, U.S. Department of Labor* – (Texas) **U.S. Labor Department’s OSHA cites Pilgrim’s Pride Corp. with repeat and serious violations for exposing workers to hazardous chemicals at Lufkin, Texas, facility.** The U.S. Department of Labor’s Occupational Safety and Health Administration December 12 cited Pilgrim’s Pride Corp. in Lufkin, Texas, with three repeat and four serious violations following a June inspection as part of the agency’s Process Safety Management Covered Chemical Facilities national emphasis program. Proposed penalties totaled \$99,000. The repeat citations issued for the process safety management standard violations included failing to inspect and test process equipment consistent with applicable manufacturers’ recommendations and good engineering practices, ensure that process equipment complies with recognized and generally accepted good engineering practices, and properly label containers holding hazard chemicals. Serious violations included failing to correct deficiencies in process equipment, ensure that process safety information pertaining to equipment includes design codes and standards, and establish and implement written procedures to manage changes of the process.

Source:

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23394

Water Sector

16. *December 12, New Jersey Jersey Journal* – (New Jersey) **Pipe repair project leaves flow of treated sewage into Hudson River visible to all.** Although few people saw it, there was nothing new about millions of gallons of treated sewage gushing into the Weehawken Cove in New Jersey daily, officials said. In November residents saw treated effluent flowing down the river bank from a row of temporary outflow pipes at the Hudson River Waterfront Walkway, near the city’s Weehawken border. Treated sewage from the Waste Water Treatment Plant would normally empty invisibly into the river below the surface from a 48-inch diameter underground sewage outflow, said the executive director of the North Hudson Regional Sewerage Authority. However, while the authority carries out a project to inspect and repair the 60-year-old outflow pipe, roughly 6 million gallons of treated sewage is being diverted temporarily overland into the river. “Everything being discharged has been treated and meets the requirements of the Department of Environmental Protection,” he said. Since the pipes run over the Hudson River Waterfront Walkway, a temporary ramp bridge has been constructed for pedestrians. The \$4.9 million project is expected to take 18 months to complete, officials said.
Source: http://www.nj.com/jjournal-news/index.ssf/2012/12/pipe_repair_project_puts_flow.html
17. *December 11, Imperial Valley Press* – (California) **Boil water order issued for Niland area.** A boil water order was issued for water customers in Niland, California, due to damage to a water transmission line, according to a press release from Golden State Water Co. December 11. Damage caused by a contractor performing work for another company prompted the California Department of Public Health, in conjunction with the Imperial County Health Department and Golden State Water Co., to advise customers in Niland to use boiled tap water or bottled water for drinking and cooking purposes as a safety precaution. This was a precautionary boil water notice, according to Golden State. The company would inform residents when tests show that water was safe to drink and residents no longer need to boil their water. The company anticipated resolving the problem within 48 hours.
Source: <http://www.ivpressonline.com/news/quicknews/ivp-boil-water-order-issued-for-niland-area-20121211,0,52609.story>
18. *December 11, U.S. Environmental Protection Agency* – (Massachusetts) **Massachusetts developers to pay a fine for Clean Water Act violations in Uxbridge.** The U.S. Environmental Protection Agency (EPA) and Albee Realty Trust resolved a penalty action for discharges of silt-laden storm water associated with development of a seven lot residential subdivision in Uxbridge, Massachusetts, in violation of the federal Clean Water Act, according to a December 11 EPA press release. Albee discharged storm water from the construction site without a permit for several years. Albee also failed to install and maintain controls sufficient to minimize discharge of pollutants to the stream. The EPA issued a complaint against the Albee Realty Trust and its trustees seeking penalties as a result of these violations June 12. However, because they are operators of a site disturbing more than one acre, Albee was required to apply for either an individual permit or coverage under a General Permit for

“Storm Water Discharges from Construction Activities.” The permit requires the use of “best management practices” to prevent erosion and sedimentation of waterways that can result from construction activities. Under the agreement, Albee will pay a penalty of \$24,000.

Source:

<http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/46bc700472e1432685257ad200518193!OpenDocument>

[\[Return to top\]](#)

Public Health and Healthcare Sector

19. *December 11, North County Gazette* – (New York) **Brooklyn doc defrauded Medicare, private insurance.** A Brooklyn board-certified colorectal surgeon who owned and operated a New York City medical clinic was sentenced to serve 30 months in prison for his role in a fraud scheme that billed Medicare and more than 10 private insurance companies for surgeries and other complex medical procedures that were never performed, the North Country Gazette reported December 11. The trial evidence showed that from January 2008 to January 2010, the doctor, who owned and operated a clinic called Colon and Rectal Care of New York P.C., defrauded Medicare and private insurance companies by billing for surgeries and medical services that he never provided. According to trial testimony, several private insurance companies began investigating the doctor after receiving complaints from patients that he had submitted claims for surgeries that he never performed. After the doctor was confronted by two insurance companies about complaints of billings for surgeries that did not happen, the evidence at trial showed that he sent letters to his patients, asking them to falsely certify in writing that they had received the phony surgeries. The indictment alleged that he submitted and caused the submission of more than \$22.6 million in false and fraudulent claims to Medicare and private insurance companies and received more than \$9 million on those claims. In addition to his prison term, he was sentenced to serve three years of supervised release, pay forfeiture of \$1,103,069, and pay restitution of \$1,103,069 to the victims of his crimes, Medicare, and numerous private insurance plans. He was found guilty of one count of health care fraud and five counts of health care false statements.

Source: http://www.northcountrygazette.org/2012/12/11/fraud_scheme/

20. *December 11, Columbia Daily Tribune* – (Missouri) **Former health tech accused of thefts.** A former University of Missouri Health Care technician and resident of Huntsville, Missouri, was arrested December 10 on suspicion of 42 counts of stealing drugs and medical supplies. A University of Missouri police captain said investigators believe the technician with MU Health’s Center for Education and Development stole nonscheduled drugs and medical supplies on several occasions between August 30 and November 23. Items allegedly were stolen from machines that store the drugs for auditing purposes and an emergency room machine that required her to enter a fake patient name. MU Health staff tracks potential discrepancies through daily data collection. Random audits allow staff to know when a drug was accessed, who accessed it, at what time, and the quantity taken, as described in court records charging the

technician.

Source: <http://www.columbiatribune.com/news/2012/dec/11/former-health-tech-accused-of-thefts/>

21. *December 10, KOB 4 Albuquerque* – (New Mexico) **ABQ Health Partners’ patient records on missing laptop.** Some patient records may be in jeopardy after ABQ Health Partners, New Mexico’s largest independent doctor’s group, reported a lost or stolen laptop, KOB 4 Albuquerque reported December 10. ABQ Health Partners sent out a letter telling patients their personal information is at risk of falling into the wrong hands. KOB 4 received a statement from ABQ Health Partners that reads, “The instance in question involved minimal patient information - no social security numbers, addresses or access to patient health records were released. Please know that ABQ Health Partners takes our patients’ privacy and confidentiality very seriously,” the letter reads. It also suggests patients may want to put a “fraud alert” on their credit files, and enclosed an instruction sheet on how to do that.
- Source: <http://www.kob.com/article/stories/S2861824.shtml?cat=500>

For another story, see item [23](#)

[\[Return to top\]](#)

Government Facilities Sector

22. *December 11, Associated Press* – (Nebraska) **Federal prosecutors charge former UNL student with hacking into sensitive university database.** A former University of Nebraska-Lincoln student is facing a federal criminal charge because prosecutors said he hacked into a database of more than 650,000 student, alumni, and employee records sometime between April 24 and May 24, the Associated Press reported December 11. Prosecutors said the former student, who was studying computer science and math, accessed a protected computer without permission. The database held records from the University of Nebraska’s campuses and the Nebraska State College System. Officials said they do not believe any sensitive information in the database was downloaded. The database included information from current and former students, university applicants, alumni, and employees dating to spring 1985. The University of Nebraska’s information security officer said in June that the university was re-evaluating its online security plans because of the incident. University officials identified the former student as a suspect during May 2011 based on the computer IP address that was used to access the system.
- Source:
<http://www.therepublic.com/view/story/dfcc32946723418aa79580899ecba0c5/NE--Nebraska-Security-Breach>
23. *December 11, The Columbia State* – (South Carolina) **Records blocked from SC’s DHEC website.** South Carolina’s Department of Health and Environmental Control (DHEC) temporarily blocked access to many public notices while the department works to ensure it does not suffer a security breach, The Columbia State reported December 11. Some public notice information was available on the Web site for at least

a month. An agency spokesman said DHEC hopes to restore public notices to its Web site sometime the week of December 10. A spokesman noted that DHEC wants to restore the information “in a way that does not present a potential vulnerability to our computer system.” The agency’s work follows a massive computer breach in September at the South Carolina Department of Revenue. The breach exposed millions of citizens’ personal information to hackers. The spokesman said his agency planned work on its Web site before the Revenue Department’s breach, but the issue at the tax department underscores the need to make sure DHEC’s data is secure. DHEC, the State’s chief environmental and health agency, keeps track of thousands of medical records and sensitive nuclear security information the agency would not want in the hands of hackers, the spokesman said.

Source: <http://www.thestate.com/2012/12/11/2552925/records-blocked-from-dhec-website.html#storylink=cpy>

For another story, see item [9](#)

[\[Return to top\]](#)

Emergency Services Sector

24. *December 12, La Crosse Tribune* – (Wisconsin) **Police gear stolen from deputy’s house.** Two firearms, a Taser, and a police radio were stolen during a burglary at a La Crosse County, Wisconsin sheriff’s deputy’s house. The deputy was not home between December 6 and December 7 when the burglary occurred. The items stolen were two guns, six loaded magazines, a yellow Taser, a silver sheriff’s department badge on a leather belt clip, a Motorola police radio, a baton, a flashlight, and a laptop. Authorities recovered the duty belt December 7 in a median at Highway 35 and Interstate 90, the chief deputy said.
Source: http://lacrossetribune.com/news/local/police-gear-stolen-from-deputy-s-house/article_72004956-441b-11e2-8308-0019bb2963f4.html
25. *December 12, Associated Press; Mason City Globe Gazette* – (Iowa) **Ex-Iowa police officer gets 10 years in prison.** A former Forest City, Iowa police officer was convicted and given up to 10 years in prison for starting a fire at the Forest City police station in October 2011 and stealing an assault rifle from a police car in November 2010. The Mason City Globe Gazette said the former officer still maintained his innocence when he was sentenced December 11 in Winnebago County District Court in Forest City. A judge convicted him of second-degree arson and second-degree burglary in a nonjury trial.
Source: <http://www.ctpost.com/news/crime/article/Ex-Iowa-police-officer-gets-10-years-in-prison-4111462.php>
26. *December 11, Associated Press* – (Illinois) **Medical helicopter hit bad weather before crash.** A medical helicopter pilot hit bad weather and crashed into a northern Illinois field, killing him and two nurses, authorities said December 11. The pilot radioed to dispatchers at Rockford Memorial Hospital that he was turning around because he had “encountered some weather” while heading to another hospital to pick

up a patient December 10, a hospital spokesman said. The Federal Aviation Administration and National Transportation Safety Board are investigating.
Source: http://www.necn.com/12/11/12/3-killed-in-medical-helicopter-crash-in-landing_nation.html?&apID=a7f54989d98a4cffa31382fdd584afbe

[\[Return to top\]](#)

Information Technology Sector

27. *December 12, IDG News Service* – (International) **U.S. law enforcement busts cybercrime rings with help from Facebook.** U.S. law enforcement agencies with the help of Facebook arrested 10 persons from various countries in connection with international cybercrime rings that targeted users on the social network. The operation is said to have identified international cybercrime rings that used various variants of a malware called Yahos. The malware infected more than 11 million computers and caused over \$850 million in losses through a Butterfly botnet, which steals computer users' credit card, bank account, and other personal identifiable information, the FBI said in a statement. The 10 persons arrested are from Bosnia and Herzegovina, Croatia, Macedonia, New Zealand, Peru, the U.K., and the U.S. Facebook's security team assisted the law enforcement agencies in the investigation by helping "to identify the root cause, the perpetrators, and those affected by the malware," the FBI said. Yahos targeted Facebook users from 2010 to October this year, and security systems were able to detect affected accounts and provide tools to remove these threats, the FBI said.
Source: <http://www.itworld.com/security/327524/us-law-enforcement-busts-cybercrime-rings-help-facebook>
28. *December 12, Threatpost* – (International) **Samsung smart TV bug allows remote access, root privileges.** Some specific models of Samsung TVs that have Wi-Fi and other advanced capabilities have a flaw that enables an attacker to take a variety of actions on the TV, including accessing potentially sensitive data, remote files and information, the drive image, and eventually gain root access to the device. The issue affects many Samsung TVs, and the researcher who discovered the problem found that he could remotely access the remote control for the TV, retrieve files located on any USB drive attached to the TV and even install malicious software. One of the founders of ReVuln, a security consultancy and research firm that discovers and sells zero-day vulnerabilities, found that the flaw in the Samsung smart TVs can be leveraged for a variety of different actions, most notably to gain root access to the vulnerable TV. ReVuln, as a matter of policy, does not disclose vulnerabilities to vendors, but the company posted a video demonstration of the exploit for the Samsung TVs in action.
Source: http://threatpost.com/en_us/blogs/samsung-smart-tv-bug-allows-remote-access-root-privileges-121212
29. *December 12, Softpedia* – (International) **North America and Europe most threatened by money-stealing Android trojans.** North American and European Android users are most likely to be targeted by malware designed to steal money. On the other hand, users in Asia are more likely to be bombarded with aggressive adware and annoying ads, according to the results of a study performed by Birdefender with the

aid of its mobile security solution between January 1 and December 1. The countries where users are most likely to be infected with money-stealing Android malware are the United States (16 percent), France (15 percent), Romania (15 percent), the United Kingdom (10 percent) and Germany (9 percent). In Asia, aggressive adware is the largest problem. While these types of elements cannot be considered malware, they mainly disrupt user experience and use up system resources, sometimes making the device unresponsive. Compared to the first half of 2012, malware and adware reports recorded an increase of 292% in the second part of the year. The most prevalent money-stealing Trojans are Android.Trojan.SMSSend and Android.Trojan.FakeInst, accounting for 67 percent of all reported global malware.

Source: <http://news.softpedia.com/news/North-America-and-Europe-Most-Threatened-by-Money-Stealing-Android-Trojans-314149.shtml>

30. *December 11, Krebs on Security* – (International) **Critical updates for Flash Player, Microsoft Windows.** Adobe and Microsoft each released security updates to fix critical security flaws in their software. Microsoft issued seven update bundles to fix at least 10 vulnerabilities in Windows and other software. Separately, Adobe pushed out a fix for its Flash Player and AIR software that address at least three critical vulnerabilities in these programs. A majority of the bugs quashed in Microsoft's patch batch are critical security holes, meaning that malware or miscreants could exploit them to seize control over vulnerable systems with little or no help from users. Among the critical patches is an update for Internet Explorer versions 9 and 10. Other critical patches address issues with the Windows kernel, Microsoft Word, and Microsoft Exchange Server. The final critical bug is a file handling vulnerability in Windows XP, Vista, and 7 that Microsoft said could allow remote code execution if a user browses to a folder that contains a file or subfolder with a specially crafted name. Adobe shipped a Flash Player update for Windows, Mac, Linux, and Android installations of the software. Adobe says that Flash Player installed with Internet Explorer 10 for Windows 8 and Google Chrome should be updated automatically; on Windows the latest version should be 11.5.502.135, and Chrome users on Windows, Mac, or Linux who have the latest version of Chrome should have version 11.5.31.5 installed.

Source: <http://krebsonsecurity.com/2012/12/critical-updates-for-flash-player-microsoft-windows/>

31. *December 11, Threatpost* – (International) **Critical vulnerability fixed in Chrome 23.** Google patched a number of security vulnerabilities in its Chrome browser December 11, including one critical flaw and three high-severity ones. The most serious vulnerability that Google fixed in Chrome 23 is a crash in the browser's history navigation mechanism. That bug, which was discovered by a member of Google's internal security team, is the only critical vulnerability fixed in the newest version of Chrome. There also are three high-severity vulnerabilities repaired in the release, including two use-after-free bugs.

Source: http://threatpost.com/en_us/blogs/critical-vulnerability-fixed-chrome-23-121112

For more stories, see items [5](#), [8](#), and [9](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <https://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

Nothing to report

[\[Return to top\]](#)

Commercial Facilities Sector

32. *December 12, WAGA 5 Atlanta* – (Georgia) **Dozens of people displaced in Atlanta apartment fire.** A December 12 fire at the Majestic Park Apartments in Atlanta left between 20 and 25 residents displaced. Atlanta firefighters were called to Building W at the complex. A spokesperson with the Atlanta Fire Department said when units arrived on the scene; heavy smoke and fire were seen on the second floor. She said efforts to put out the fire were delayed because no water was available at the first hydrant they tried to use. Once they were able to get water, crews got the fire under control. Authorities said six units were destroyed, and another heavily damaged. Source: <http://www.myfoxatlanta.com/story/20323897/several-people-displaced-in-atlanta-apartment-fire>
33. *December 12, Associated Press* – (Missouri) **Hotel fire in Kansas City suburb displaces about 50 people.** A hotel fire in Liberty, Missouri, forced the evacuation of about 50 people December 12. Fire officials said one firefighter was treated and released for injuries after falling from a second-floor balcony at the Day's Inn. Two people were rescued from the motel's second floor. A damage estimate was not immediately available but authorities said up to eight rooms were heavily damaged. Source: <http://www.kspr.com/news/ky3-hotel-fire-in-kansas-city-suburb-displaces-about-50-people-20121212,0,4326062.story>
34. *December 12, Clark County Columbian; Associated Press; Los Angeles Times* – (Oregon) **Three dead, one injured in shooting at Clackamas Town Center.** A suspect killed two people and wounded another before taking his own life December 11 at the Clackamas Town Center southeast of Portland, Oregon. Another victim was taken by helicopter to a hospital in Portland where she remained in serious condition, but was expected to survive, authorities said. In a press briefing, the Clackamas County sheriff said 4 SWAT teams searched the 1.4 million-square-foot mall for people who barricaded themselves for safety. An estimated 10,000 people were at the mall at the time of the shooting, he said. Witnesses said a gunman armed with a semi-automatic weapon opened fire after entering the mall through the Macy's department store

entrance, then moved to the food court, where he continued shooting. About 100 officers descended on the mall within minutes of the shooting. A lieutenant with the sheriff's office said the gunman acted alone, something that was uncertain after the shooting. He said the suspect apparently died of a self-inflicted gunshot wound. Sunnyside Road and southbound lanes of Interstate 205 were temporarily closed as officials locked down the mall and established a perimeter to contain the scene. Three helicopters were brought in to evacuate victims. Two were released and the third remained on standby. TriMet announced that neither the MAX Green Line nor bus lines 28, 29, 30, 31, 71, 72, 79, 152, 155, and 156 would stop at the closed mall December 12, and that the CTC Transit Center park-and-ride garage would be closed. Source: <http://www.columbian.com/news/2012/dec/11/shooting-reported-clackamas-town-center/>

35. *December 11, Columbia Daily Tribune* – (Missouri) **Fulton auto shop damaged by fire.** A Fulton, Missouri automotive shop was destroyed by fire December 10 resulting in an estimated \$200,000 in damages, the Columbia Daily Tribune reported December 11. Investigators with the Fulton Fire Department and Missouri Fire Marshal's Office were unable to confirm an origin or cause fire at the shop because damage was too extensive, said a Fulton Fire Department engineer. Investigators estimated \$200,000 in damages in light of equipment, tools, and vehicles stored in the metal structure. Firefighters arrived on scene to find heavy smoke and flames shooting through the roof of the commercial structure. The Columbia Fire Department and the Central Callaway Fire Protection District also responded. A wood shop and wood stoves located within the structure contributed to the fire as fuel. Metal roofing that fell on the fire made it difficult for firefighters to spray water on the burning structure. Source: <http://www.columbiatribune.com/news/2012/dec/11/fulton-auto-shop-damaged-by-fire/>

[\[Return to top\]](#)

National Monuments and Icons Sector

Nothing to report

[\[Return to top\]](#)

Dams Sector

36. *December 12, Point Pleasant Register* – (West Virginia) **Floodwall drain lines need work.** In its ongoing effort to comply with new federal regulations born out of Hurricane Katrina, the City of Point Pleasant, West Virginia, has until November 2013 to correct some problems with drain lines going under the floodwall. The city's street commissioner spoke about the recent outcome of a floodwall pipeline inspection at a meeting of the Point Pleasant City Council the week of December 10. The inspection was done by Pipeline and Drainage Consultants from Burlington, Kentucky, for \$16,080. Part of this inspection included a video inspection of the main storm drain lines, sanitary sewer lines, pump lines, and Toe Drains. He said the video revealed

repairs were needed on the line running under the floodwall on First Street. Also revealed was sludge in the lines near Pump House One near Southern States, though the lines near Pump House One are otherwise in satisfactory condition. If the city does not get these problems fixed, anyone in Point Pleasant with a loan insured by the Federal Deposit Insurance Corporation would be forced to have flood insurance. The city spent around \$50,000 in meeting new federal, unfunded mandates which grew out of the failure of levees in New Orleans after Hurricane Katrina.

Source: http://www.mydailyregister.com/view/full_story/21097058/article-Floodwall-drain-lines-need-work

37. *December 12, Bennington Banner* – (Vermont) **Flood-damaged wall under repair.** Work was underway to stabilize a flood wall along the Roaring Branch in Vermont, which was battered in 2011 by Tropical Storm Irene, the Bennington Banner reported December 12. The concrete flood wall along County Street sustained some damage in August 2011. Fast-moving flood water pounded the wall hour after hour, and debris slammed into the wall. The wall stood strong, but sink holes emerged on the land side that town workers quickly filled. After the storm the wall and sink holes were inspected by the U.S. Army Corps of Engineers. The repair work — paid for entirely by the Corps — began the week of December 3. The repair plan, mostly created by the town’s engineering firm Milone & MacBroom, involves drilling into a broad base below the earth, according to the town’s planning director. Concrete will then be pumped under high pressure into those holes to fill any voids underneath. The holes will then be sealed back up, he said. The project also includes replacing large rocks, or rip rap, along the flood wall to help protect it. The town has also completed repairs further down river to the levee that runs alongside the Mount Anthony Union High School property. The earthen wall sustained “severe damage,” but was quickly repaired by the town according to Corps standards, he said. That work, which cost between \$200,000 and \$400,000, was part of a reimbursement request the town has pending with the Federal Emergency Management Agency. The work was expected to be completed in 10 to 14 days.

Source: http://www.benningtonbanner.com/news/ci_22172856/flood-damaged-wall-under-repair

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2341

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.