



## Daily Open Source Infrastructure Report 18 December 2015

### Top Stories

- The former chief executive officer of Retrophin Inc., December 17 was charged with committing fraud after misappropriating over \$1 million from 2 hedge funds he founded, and making false claims to investors, among other misconducts. – *U.S. Securities and Exchange Commission* (See item [2](#))
- A former portfolio manager at Canarsie Capital LLC was charged December 16 for secretly subjecting investors to massive risk, causing the fund to lose \$56.5 million and collapse. – *U.S. Securities and Exchange Commission* (See item [4](#))
- Two Clark County residents were indicted December 16 for felony theft charges after the two vandalized \$116,000 worth of lighting systems and stole 34,300 feet of copper wire across Interstate 1-64 in Kentucky. – *WTVQ 40 Lexington* (See item [9](#))
- A severe storm that moved across North Dakota and South Dakota December 16 caused power outages to hundreds of homes, businesses, and schools, prompted travel alerts, and forced Ellsworth Air Force Base to close. – *Associated Press* (See item [12](#))

---

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

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

#### SUSTENANCE and HEALTH

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

#### SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

#### FEDERAL and STATE

- [Government Facilities](#)
  - [Emergency Services](#)
-

## Energy Sector

1. *December 16, Farmington Daily Times* – (New Mexico) **PRC approves San Juan Generating Station plan.** The New Mexico Public Regulation Commission approved a plan December 16 to shut down 2 of 4 generating units at the San Juan Generating Station to help bring the plant into compliance with Federal haze regulations. The remaining units at the plant will be retrofitted with selective non-catalytic reduction technology and will help replace the lost generating capacity in tandem with other energy sources by December 2017.

Source: <http://www.daily-times.com/story/news/local/four-corners/2015/12/16/prc-approves-san-juan-generating-station-plan/77368644/>

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

## Chemical Industry Sector

Nothing to report

## Nuclear Reactors, Materials, and Waste Sector

Nothing to report

## Critical Manufacturing Sector

Nothing to report

## Defense Industrial Base Sector

Nothing to report

## Financial Services Sector

2. *December 17, U.S. Securities and Exchange Commission* – (National) **SEC charges former CEO with fraud.** The U.S. Securities and Exchange Commission charged the former chief executive officer (CEO) of Retrophin Inc., a pharmaceutical company, December 17 with misappropriating over \$1 million from 2 hedge funds he founded, MSMB Capital Management LP and MSMB Healthcare LP, and for making material misrepresentations to investors, among other misconduct. The former CEO worked with two other co-conspirators to mislead investors and executives about the hedge funds' size and performance, which resulted in millions in losses.  
Source: <http://www.sec.gov/news/pressrelease/2015-282.html>
3. *December 16, Charleston Post and Courier* – (South Carolina; Georgia) **Summerville mortgage fraud probe nets new indictment; losses totaled \$23 million.** Federal authorities announced that 2 suspects from Summerville were charged December 15 for their roles in a \$45 million mortgage loan scheme in South Carolina and Georgia involving 70 properties and losses of more than \$23 million. Three others pleaded

guilty in connection to the scheme based off real estate and mortgages businesses in the town.

Source: <http://www.postandcourier.com/article/20151216/PC05/151219525/1005/>

4. *December 16, U.S. Securities and Exchange Commission* – (New York) **SEC: Hedge fund adviser lied to investors.** The U.S. Securities and Exchange Commission announced December 16 that a former portfolio manager at Canarsie Capital LLC in New York was charged for making false and misleading statements to investors about the fund's performance, lying to the fund's prime brokers to avoid margin calls, and for liquidating all of the long positions in a long/short equity portfolio, causing the fund to lose about \$56.5 million and collapse.  
Source: <http://www.sec.gov/news/pressrelease/2015-281.html>
5. *December 16, Federal Bureau of Investigation, Knoxville* – (Tennessee) **Arrest and indictment of armed bank extortionists.** The FBI announced December 16 that two suspects were arrested in North Carolina for their roles in a series of robberies at three Tennessee banks, including the Y-12 Federal Credit Union in Oak Ridge, SmartBank in Knoxville, and Northeast Community Credit Union in Elizabethton from April to October.  
Source: <https://www.fbi.gov/knoxville/press-releases/2015/arrest-and-indictment-of-armed-bank-extortionists>

For another story see item [16](#)

## **Transportation Systems Sector**

6. *December 17, Douglas County Sentinel* – (Georgia) **Teen killed in Hwy. 5 collision Wednesday evening.** Highway 5 in Douglas County was closed for approximately 3 hours December 16 while officials investigated the scene of a fatal 2-vehicle crash that killed 1 passenger and seriously injured another.  
Source: [http://www.douglascountysentinel.com/news/teen-killed-in-hwy-collision-wednesday-evening/article\\_828ae26e-a45c-11e5-9949-37ea8eac482f.html](http://www.douglascountysentinel.com/news/teen-killed-in-hwy-collision-wednesday-evening/article_828ae26e-a45c-11e5-9949-37ea8eac482f.html)
7. *December 16, Vero Beach Press Journal* – (Florida) **Carjacking ends in rollover crash that closed I-95 west of Palm City for 3 hours.** Interstate 95 in Martin County was shut down for 3 hours after a car-jacking chase led to a crash that sent 3 people to the hospital.  
Source: <http://www.tcpalm.com/news/martin-county/rollover-crash-closes-sb-i-95-in-palm-city-2705c428-ec24-2c18-e053-0100007f1b88-362626361.html>
8. *December 16, Los Angeles Times* – (California) **Several lanes of Interstate 5 through the Grapevine closed because of chemical spill.** Several southbound lanes of Interstate 5 in Los Angeles were closed for several hours December 16 while HAZMAT crews worked to clean the wreckage from an overturned semi-truck that spilled ethyl alcohol, sodium chloride, and various other chemicals. Officials reported that the lanes will remain closed until the cleanup and damage repairs are completed.  
Source: <http://www.latimes.com/local/lanow/la-me-ln-interstate-5-closed-chemical->

[spill-20151216-story.html](http://www.wtvq.com/2015/12/16/clark-co-man-woman-indicted-in-copper-wire-thefts-on-highways/)

9. *December 16, WTVQ 40 Lexington* – (Kentucky) **Clark Co. man, woman indicted in copper wire thefts on highways.** Two Clark County residents were indicted December 16 with seven counts of theft and seven counts of first-degree criminal theft after an investigation revealed the two vandalized \$116,000 worth of lighting systems and cut and removed about 34,300 feet of copper wire across Interstate 1-64 in Bath and Carter counties, Woodford County, and Clark County from October – November.  
Source: <http://www.wtvq.com/2015/12/16/clark-co-man-woman-indicted-in-copper-wire-thefts-on-highways/>

For another story, see item [12](#)

## **Food and Agriculture Sector**

Nothing to report

## **Water and Wastewater Systems Sector**

Nothing to report

## **Healthcare and Public Health Sector**

See item [2](#)

## **Government Facilities Sector**

10. *December 17, Reuters* – (Indiana) **Schools around U.S. receive hoax threats; two arrested in Indiana.** Officials announced that two students were arrested for making social media threats against high schools in Danville and Plainville, forcing school closures December 17. School districts in Texas and Florida also received threats of violence similar to those made against schools in New York and Los Angeles December 15, but were later determined a hoax.  
Source: <http://www.msn.com/en-us/news/us/two-indiana-school-districts-shut-down-amid-threats-toward-schools/ar-BBnEnAM?li=BBnb7Kz>
11. *December 17, San Bernardino Sun* – (California) **San Bernardino Valley College students get back to campus after bomb threat.** San Bernardino Valley College in California reopened December 16 after the college was shut down December 14 – 15 following a credible bomb threat. Police are investigating the source of the threat and deemed the campus safe after nothing suspicious was found.  
Source: <http://www.sbsun.com/general-news/20151216/san-bernardino-valley-college-students-get-back-to-campus-after-bomb-threat>
12. *December 16, Associated Press* – (North Dakota; South Dakota) **Storm leads to power outages, closed schools in Dakotas.** A severe storm that moved across North Dakota and South Dakota December 16 knocked out power to hundreds of homes and businesses, closed schools, prompted travel alerts, and forced Ellsworth Air Force Base

in South Dakota to close due to poor road conditions.

Source: [http://rapidcityjournal.com/news/local/storm-leads-to-power-outages-closed-schools-in-dakotas/article\\_454ebc40-296d-5997-844d-f3b77517cd49.html](http://rapidcityjournal.com/news/local/storm-leads-to-power-outages-closed-schools-in-dakotas/article_454ebc40-296d-5997-844d-f3b77517cd49.html)

13. *December 16, Bellingham Herald* – (Washington) **Ferndale High School evacuated after bomb threat.** Students from Ferndale High School in Washington were evacuated and classes were dismissed December 16 after a student discovered a bomb threat on social media and reported it to school officials. Police searched the campus and deemed it safe after nothing suspicious was found.  
Source: <http://www.bellinghamherald.com/news/local/crime/article50062660.html>
14. *December 16, WCCO 4 Minneapolis* – (Minnesota) **Officials: 4 students injured in bus rollover in Hackensack.** Four students were transported to an area hospital with injuries after their school bus slid off the roadway and overturned in Hackensack, Minnesota, December 16.  
Source: <http://minnesota.cbslocal.com/2015/12/16/officials-1-student-injured-in-bus-accident-in-hackensack/>
15. *December 16, WABC 7 New York City* – (New York) **Mace blamed for fumes that forced West Babylon school evacuation, hospitalizations.** Authorities determined that mace was the source of fumes that sickened 35 students and faculty members at West Babylon High School on Long Island December 15, after an investigation found that 2 students sprayed mace in the school hallway.  
Source: <http://abc7ny.com/education/mace-blamed-for-fumes-that-forced-li-school-evacuation-hospitalizations/1123765/>
16. *December 16, San Francisco Bay City News* – (California) **Former ABAG financial services director guilty of fraud, admits stealing nearly \$3.9 million.** A former financial services director for the Association of Bay Area Governments, a regional urban planning agency, pleaded guilty in Federal court in San Francisco December 15 to embezzling close to \$3.9 million from funding allocated by the agency for public works projects in California between 2011 and 2015.  
Source:  
[http://www.mercurynews.com/crime-courts/ci\\_29262897/former-abag-financial-services-director-guilty-fraud-admits](http://www.mercurynews.com/crime-courts/ci_29262897/former-abag-financial-services-director-guilty-fraud-admits)

## **Emergency Services Sector**

Nothing to report

## **Information Technology Sector**

17. *December 16, Softpedia* – (International) **XRTN ransomware discovered, currently undecryptable.** A researcher from Bleeping Computer's released a report on the XRTN ransomware detailing how the malware infects a computer system by sending email attachments, such as malicious Word documents and batch files that are encoded with JavaScript commands, to a victim's corporate or personal email, that if opened and

- downloaded, attackers can execute the JavaScript commands to run batch files that will encrypt personal data files and add the .xrtm extension. All files are encrypted with an RSA-1024 key, which can only be decrypted with a private key held by the attacker.  
Source: <http://news.softpedia.com/news/xrtm-ransomware-discovered-currently-undecryptable-497739.shtml>
18. *December 16, Softpedia* – (International) **Four Network Management Systems vulnerable to SQLi and XSS attacks.** Two security researchers discovered six vulnerabilities in four Network Management Systems (NMS) that allow attackers to gain access to applications and use the affected system to carry out future attacks via four cross-site scripting (XSS) flaws and two SQL injection (SQLi) flaws, which enables hackers to access a user's session information, through the management interface, breach the underlying database, steal information about all connected devices, and escalate privileges over the server itself.  
Source: <http://news.softpedia.com/news/four-network-management-systems-vulnerable-to-sqli-and-xss-attacks-497735.shtml>
19. *December 16, IDG News Service* – (International) **Grub2 bootloader flaw leaves locked-down Linux computers at risk.** Two researchers from the Cybersecurity Group at Universitate Politehnica de Valencia found an integer underflow vulnerability in Grand Unified Bootloader2 (GRUB2), a boot loader for Linux systems, that can be triggered by pressing the backspace key 28 times when the bootloader asks for a user's credentials, allowing unauthorized access to a powerful shell which can enable hackers to rewrite the Grub2 code loaded in the RAM and bypass the authentication checkpoint. Once an attacker penetrates the bootloader, hackers can destroy data on the disk and install malware to steal authentic users' encrypted home folder data. The vulnerability exist in all versions of GRUB2 from 1.98 released December 2009 to the current 2.02.  
Source: [http://www.computerworld.com/article/3015995/security/grub2-bootloader-flaw-leaves-locked-down-linux-computers-at-risk.html#tk.rss\\_security](http://www.computerworld.com/article/3015995/security/grub2-bootloader-flaw-leaves-locked-down-linux-computers-at-risk.html#tk.rss_security)
20. *December 15, The Register* – (International) **Web host Moonfruit defies Armada DDoS crew... by (temporarily) defeating itself.** United Kingdom-based Web host, Moonfruit was back online after pulling its own Web site and many of its customers' Web sites offline for approximately twelve hours while researchers upgraded the company's defenses and advised users to update settings following a December 10 denial-of-service (DDoS) attack by the Armada Collective Crew that shut down the company's Web site for 45 minutes. The company stated they were making significant infrastructure changes to prevent future DDoS attacks.  
Source: <http://www.v3.co.uk/v3-uk/news/2439205/moonfruit-takes-thousands-of-websites-offline-after-cyber-attack-threat>

## Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto: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: <http://www.it-isac.org>

### Communications Sector

21. *December 16, Eureka Times-Standard* – (California) **AT&T vows to upgrade North Coast network after outages.** AT&T Inc. officials announced December 16 that it will be upgrading its North Coast Network by 2016 to prevent single point failures and to reduce outage impacts on local communities, such as wire cuts and Internet service failures, by reprogramming its equipment to route service traffic over diverse fiber paths.  
Source: <http://www.times-standard.com/general-news/20151216/att-vows-to-upgrade-north-coast-network-after-outages>

### Commercial Facilities Sector

22. *December 17, WPVI 6 Philadelphia* – (Pennsylvania) **Flames destroy church in Wilmington, Delaware; 2<sup>nd</sup> fire in 2 weeks.** The New Jerusalem Missionary Baptist Church in Wilmington, Pennsylvania sustained extensive damage December 16 after a two-alarm fire began in the church and spread to six adjacent homes. One firefighter sustained minor injuries and FBI officials are investigating whether the incident was a hate crime after the incident was the second church fire in two weeks.  
Source: <http://6abc.com/news/another-fire-destroys-wilmington-church/1125701/>
23. *December 16, Knoxville News Sentinel* – (Tennessee) **Carbon monoxide leak causes apartment evacuation.** Oak Ridge officials reported December 15 that the Rolling Hills Apartment complex evacuated its three-story building after police received complaints of headaches and nausea due to a carbon dioxide leak caused from a faulty boiler. Twenty residents were displaced and one person was sent to the hospital while the Oak Ridge Utility District made repairs to the boiler.  
Source: <http://www.knoxnews.com/news/local/carbon-monoxide-leak-causes-apartment-evacuation-270c717d-4506-1f04-e053-0100007f72d3-362708071.html>
24. *December 16, Asbury Park Press* – (New Jersey) **Police find \$1M in stolen goods, arrest accused burglar.** Little Silver Police arrested and charged a man in Neptune December 10 for six counts of burglary, six counts of theft, and six counts of receiving stolen property, among other charges, after an investigation revealed that the man stole more than \$1 million in stolen goods from 2012 – 2015.  
Source: <http://www.app.com/story/news/crime/jersey-mayhem/2015/12/16/police-find-stolen-goods-arrest-accused-burglar/77432344/>
25. *December 16, KUSA 9 Denver* – (Colorado) **Card skimmers found at three Colorado Safeway stores.** Safeway Inc. officials reported December 16 that card skimming

devices were found at checkout lanes at its grocery stores in Lakewood, Denver, and Conifer following routine inspections conducted by store employees early November. Safeway Inc. officials notified banks and advised customers to monitor their bank accounts for fraudulent activity.

Source: <http://www.9news.com/story/money/personal-finance/consumer/2015/12/16/card-skimmers-found-at-three-colorado-safeway-stores/77443874/>

For additional stories, see items [12](#) and [17](#)

## **Dams Sector**

Nothing to report



**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 <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the <a href="#">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="#">Get e-mail updates when this information changes</a> .
Removal from Distribution List:	Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a> .

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@hq.dhs.gov](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.