Daily Open Source Infrastructure Report
10 December 2012

Top Stories

- Researchers December 6 unleashed proof-of-concept code that would allow an attacker to effectively write himself a check from the victim organization's accounting software. They said the same types of attacks could also be aimed against a variety of accounting packages. – *Dark Reading* (See item 3)
- Grease and rags from a residential neighborhood clogged a 15-inch plastic sewer line in San Antonio December 4, causing 63,000 gallons of sewage to overflow. – *San Antonio Express-News* (See item 7)
- Two separate reports released December 6 showed that 94 percent of U.S. healthcare organizations have been hit by at least 1 data breach, and close to half suffered more than 5 breaches in the past 2 years. – *Dark Reading* (See item 16)
- According to Microsoft's Malware Protection Center, the Necurs malware has been spotted on 83,427 unique computers in November alone. Experts revealed that the malware might even be capable of disabling Microsoft Security Essentials' real time protection. – *Softpedia* (See item 24)

Fast Jump Menu

Energy Sector

Nothing to report

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

1. *December 7, Associated Press* – (Michigan) **Fermi 2 nuclear power plant still down as repairs continue.** DTE Energy said it may take months before the Fermi 2 nuclear power plant returns to full power because of substantial repairs needed on a reactor water pump. The plant, located next to Lake Erie in Frenchtown Township, Michigan, has been running at reduced power since July and has been off-line since November 7. "It's a matter of taking the generator apart, and that's a very large, complex piece of machinery, determining the cause, repairing the problems and then getting it reassembled," a DTE spokesman told WWJ 950 AM Detroit. After disassembling portions of the massive generator, the spokesman said workers had to find the small area that was allowing hydrogen gas from one part of the cooling system to leak into part of the system that is water-cooled, which decreases the system's effectiveness. The spokesman said although the plant is shut down, people in the surrounding area should not worry because the plant is in a safe, stable condition.
   Source: http://detroit.cbslocal.com/2012/12/07/fermi-2-nuclear-power-plant-could-remain-off-line-for-months/

[Return to top]

Critical Manufacturing Sector

2. *December 7, U.S. Department of Transportation* – (National) **NHTSA recall notice - 2013 Ford Fusion headlamp projector coating.** Ford announced December 7 the recall of 19,106 model year 2013 Fusion vehicles manufactured from February 3, 2012 through October 20, 2012 for failing to conform to the requirements of Federal Motor Vehicle Safety Standard (FMVSS) number 108, "Lamps, Reflective Devices, and Associated Equipment." The affected vehicles may not have had the low beam headlamp projector coating properly cured during its manufacturing process. An improperly cured projector coating will become hazy through operation, over time, reducing the brightness of the low-beam lamp. This may decrease driver visibility and increase the risk of a vehicle crash. Ford will notify owners, and dealers will replace the headlamp assembly.
   Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V553000&summary=true&prod_id=1700810&PrintVersion=YES

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

3. *December 6, Dark Reading* – (International) **'Project Mayhem' hacks accounting software.** Researchers December 6 unleashed proof-of-concept code that would allow an attacker to basically write himself a check from the victim organization's account. The Python-based tool is just one example of the type of advanced financial fraud that could be perpetrated against accounting applications and databases, according to SecureState researchers, who at Black Hat Abu Dhabi demonstrated their tool and findings on threats to accounting software. They focused their efforts on Microsoft's Dynamics Great Plains application, but they said the same types of attacks could also be aimed at other accounting packages. No vulnerabilities were discovered or exploited in the Microsoft product. The Mayhem script detects that the Microsoft software is running, and creates a backdoor for the attacker to remotely make SQL queries and commit all types of financial fraud. "It doesn't even need to install a traditional piece of [trojan] backdoor malware like" most financial fraud malware does today, said the manager of SecureState's penetration testing team. "We compare it with a banking trojan that hijacks [automated clearing house] ACH and wire transfers without the user's knowledge, but this time we're looking at the accounting system instead of the online banking session," he said. Microsoft's accounting program is not the only

potential victim. The manager said the same concept could be applied to MAS 90, Peachtree, Oracle, and SAP.
Source: http://www.darkreading.com/database-security/167901020/security/application-security/240144003/project-mayhem-hacks-accounting-software.html

4. *December 6, Associated Press* – (Colorado) **Federal fraud charges in Colorado bank failure.** A former New Frontier Bank loan officer is facing federal fraud charges involving millions of dollars in the 4 years prior to the Greeley, Colorado bank's shutdown by State regulators in 2009. The man appeared in U.S. District Court December 5. He was the chief loan officer at New Frontier, which had $2 billion in assets before lending practices turned it into one of the country's most expensive bank failures in 2009, costing the Federal Deposit Insurance Corp. $670 million. The man was responsible for making more than $20 million in loans to borrowers in return for $4.3 million used to purchase New Frontier Bankcorp stock. He is also accused of trying to pocket $160,000 in illegally obtained money.
Source: http://www.sfgate.com/news/crime/article/Federal-fraud-charges-in-Colorado-bank-failure-4096795.php

5. *December 6, IDG News Service* – (International) **Former Anonymous member convicted in attacks against PayPal, MasterCard, Visa.** A U.K. man was convicted for his involvement in a series of distributed denial-of-service (DDoS) attacks launched by the hacktivist group Anonymous against PayPal, MasterCard, Visa, and other companies in 2010. The man was convicted December 6 in a London court on one count of conspiracy to impair the operation of computers, the U.K.'s Crown Prosecution Service said in a blog post. The man, who used the online handle "Nerdo," was arrested in January 2011 and was charged in September 2011 with computer-related offenses in relation to Anonymous' "Operation Payback" attack campaign. DDoS attacks launched as part of "Operation Payback" originally targeted companies and organizations from the music industry. However, the campaign later switched its focus toward PayPal, MasterCard, Visa, and other financial companies. Three other men arrested in the U.K. in connection with the same attacks pleaded guilty earlier in 2012 to one count each of conspiracy to impair the operation of computers. According to the Crown Prosecution Service, the DDoS attacks cost PayPal, MasterCard, Visa, the British Recorded Music Industry, Ministry of Sound, and the International Federation of the Phonographic Industry $5.6 million in additional staffing, software, and loss of sales.
Source:
http://www.computerworld.com/s/article/9234434/Former_Anonymous_member_convicted_in_attacks_against_PayPal_MasterCard_Visa?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+N

[Return to top]

Transportation Sector

6. *December 7, Associated Press* – (California) **3 arrested for robbing Bay Area bridge toll takers.** The California Highway Patrol (CHP) said three Vallejo men were arrested on suspicion of robbing toll takers at the Carquinez Bridge. CHP officials said December 6 the three suspects are accused of targeting toll takers at the bridge between Crockett and Vallejo three times between late 2011 and May 2012. CHP officials said the toll takers were robbed of between $5,000 and $6,000 by a masked passenger, sometimes flashing a gun from the back seat of a car. The CHP is investigating the involvement of as many as seven more people. Investigators used surveillance video and stolen car reports to identify the robbers. The suspects were booked at a county jail on suspicion of robbery.
Source: http://www.sfgate.com/news/crime/article/3-arrested-for-robbing-Bay-Area-bridge-toll-takers-4098186.php

7. *December 7, Associated Press* – (New York) **Bus driver not guilty of manslaughter in NY crash.** A casino bus driver at the helm of a New York crash that killed 15 people in 2011 was found not guilty of manslaughter and criminally negligent homicide December 7. He was found guilty on one count of aggravated unlicensed operation of a motor vehicle. The defense attorney said he was well-rested and the crash was the result of a tractor-trailer that swiped the bus and drove off, causing the bus driver to lose control. The bus was driving from a Connecticut casino to New York's Chinatown when it crashed March 12, 2011. Authorities said the speeding bus ran off the highway, hit a guardrail, and then toppled.
Source: http://www.seattlepi.com/news/crime/article/Bus-driver-not-guilty-of-manslaughter-in-NY-crash-4098542.php

8. *December 6, Charlotte Observer* – (North Carolina) **Man charged with carrying gun at Charlotte airport.** A South Carolina man faces a misdemeanor charge of carrying a concealed weapon after police said he attempted to take a gun through a security checkpoint at Charlotte-Douglas International Airport. The man was stopped by Transportation Security Administration (TSA) officials November 27 when he attempted to conceal a Colt .45 pistol in his carry-on, Charlotte-Mecklenburg police (CMPD) said. TSA officials confiscated the gun, and CMPD officers arrested the man. He was booked in a county jail and was set to appear in court January 18, 2013.
Source: http://www.charlotteobserver.com/2012/12/06/3708756/man-charged-with-carrying-gun.html

9. *December 5, Reuters* – (International) **Boeing 787 in emergency landing as inspections ordered.** On the same day one of its new Dreamliners made an emergency landing because of a mechanical problem, Boeing said U.S. regulators had ordered the entire fleet of 787 jets to be inspected for a possible fuel line problem, Reuters reported December 6. A brand new United Airlines 787 Dreamliner with 184 people aboard was forced to divert and make an emergency landing in New Orleans December 4 after experiencing a mechanical problem on a flight from Houston to Newark, New Jersey. Boeing said December 4 the U.S. Federal Aviation Administration (FAA) was requiring inspections of all 787s in service to confirm that fuel line connectors had been

properly installed. The checks were recommended after two non-U.S. carriers experienced fuel leaks. Japan's All Nippon Airways (ANA), Boeing's Dreamliner launch customer, said December 5 it had reported the leak to the FAA and Boeing. The ANA spokesman said the carrier found the fuel leak on October 23. The FAA requirement, due to be issued December 12 in an airworthiness directive, "makes mandatory inspections already recommended by Boeing," the company said in a statement.
Source: http://www.reuters.com/article/2012/12/05/uk-united-787-diversion-idUSLNE8B400M20121205

[Return to top]

Postal and Shipping Sector

10. *December 7, Associated Press* – (Texas) **Iranian man gets prison for Texas mail, ID theft.** An Iranian man living in the Houston area was sentenced to more than 20 years in prison for stealing mail, setting up fake identities, and financial fraud, the Associated Press reported December 7. Prosecutors said he took advantage of the U.S. postal system and about 500 people were affected by the scheme. A jury in April convicted him of four counts of bank fraud, one count of possession of stolen mail, and three counts of aggravated identity theft. The man has been in custody since 2010 when authorities discovered stolen mail, fake credit cards, and cash in his apartment.
Source: http://www.chron.com/news/texas/article/Iranian-man-gets-prison-for-Texas-mail-ID-theft-4099198.php

11. *December 6, Associated Press* – (Ohio) **Columbus postal worker to plead guilty to mail theft.** A U.S. Postal Service worker will plead guilty to charges accusing him of stealing cash and gift cards from mail at a Columbus, Ohio processing center and assaulting officers, the Associated Press reported December 6. Federal authorities said Postal Service agents saw the worker open envelopes and remove the contents while sorting mail in June at the center and put mail in his sock and down his pants. Agents said he punched and bit them when they arrested him. Documents filed December 6 in federal court in Columbus say he will plead guilty to 71 counts of mail theft, 12 counts of receiving stolen mail, and 2 counts of assaulting a federal officer. Investigators said they recovered 71 first-class letters, 20 gift cards, and $341 in cash on the former worker after searching him.
Source: http://www.cantonrep.com/newsnow/x1233655866/Columbus-postal-worker-to-plead-guilty-to-mail-theft

[Return to top]

Agriculture and Food Sector

12. *December 6, Food Safety News* – (National) **Frozen chicken recalled nationwide for pieces of plastic.** Suzanna's Kitchen is recalling approximately 35,800 pounds of breaded chicken products because they may contain pieces of plastic, the U.S. Department of Agriculture's Food Safety and Inspection Service said December 6. The

recalled products include cases containing 12-ounce cartons of Freebird Fully Cooked Chicken Nuggets with a use-by date of March 15, 2014, 12-ounce cartons of Freebird Fully Cooked Gluten Free/Soy Free Chicken Patties with a use-by date of September 6, 2013, and 10-pound bulk cases of Fully Cooked Chicken Nuggets with a use-by date of March 15, 2014. The recalled products were shipped to a food service distributor in California for further distribution. The recalled products were produced March 15, 2012, and September 6, 2011.
Source: http://www.foodsafetynews.com/2012/12/frozen-chicken-recalled-nationwide-for-pieces-of-plastic/#.UMHk1eTAcWs

13. *December 6, KRQE 13 Albuquerque* – (New Mexico; Colorado) **Loaded pistol found packed in frozen meat.** An Albertsons employee in Roswell, New Mexico, found a handgun with ammunition placed inside a frozen meat package December 5. The semi-automatic and its ammunition was turned over to police. The Roswell Police Department said that the particular model of gun is rarely seen in the area. According to the police report, the meat package came from the Swift Packing Plant in Greeley, Colorado, and the date on the package was June 8, 2011. Police said the pistol was not reported stolen. The Albertsons supervisor told police there was an indention in the box where the gun was packed in with the frozen meat.
Source: http://www.krqe.com/dpp/news/crime/loaded-pistol-found-packed-in-frozen-meat

[Return to top]

Water Sector

14. *December 7, Associated Press* – (North Carolina) **Animal waste from dairy farm flows into North Carolina river.** North Carolina environmental officials said animal waste from a dairy farm in Fletcher, North Carolina, flowed into the French Broad River. The Asheville Citizen-Times reported that officials were called December 4 by the local riverkeeper. An inspector with the Division of Water Quality said waste was entering the river from a storage pond at about 11,000 gallons an hour. Officials reported a high fecal coliform bacteria level in that part of the river, and that they were not sure how long the pond had been overflowing. The farm owner and inspectors managed to stop the flow December 4.
Source: http://myfox8.com/2012/12/07/animal-waste-from-dairy-farm-flows-into-north-carolina-river/

15. *December 6, San Antonio Express-News* – (Texas) **63,000-gallon sewer spill on Northeast Side.** Grease and rags from a residential neighborhood clogged a 15-inch plastic sewer line in San Antonio December 4, causing 63,000 gallons of sewage to overflow. The San Antonio Water System (SAWS) was notified of the spill when a resident called in a smell complaint. Crews cleared the PVC sewer line that night. They spent December 5 vacuuming up a pool of sewage and spreading disinfectant. SAWS is asking City Council to approve an 11.3 percent rate increase, most of which will go toward improving the utility's sewer pipe inspection, cleaning, and replacement program.

Source: http://www.mysanantonio.com/living_green_sa/article/63-000-gallon-sewer-spill-on-Northeast-Side-4093620.php

[Return to top]

Public Health and Healthcare Sector

16. *December 6, Dark Reading* – (National) **Most healthcare organizations suffered data breaches.** Two separate reports released December 6 showed that 94 percent of U.S. healthcare organizations have been hit by at least 1 data breach and close to half suffered more than 5 breaches in the past 2 years. The estimated cost to the healthcare industry of these breaches is now at an average of $7 billion per year, a 15 percent increase over the past three years, according to the Third Annual Benchmark Study on Patient Privacy & Data Security study by The Ponemon Institute, which was commissioned by ID Experts. According to a second unrelated report from The Health Information Trust Alliance (HITRUST), there were some 500 data breaches at U.S. healthcare organizations from 2009 to the present, with 21 million personal records exposed — an estimated cost of $4 billion in damages. HITRUST included only breaches affecting 500 or more individuals, and says the numbers, which come from U.S. Department of Health and Human Services (HHS) data, signal little improvement in preventing breaches. More than 60 percent of those breaches came at smaller-sized physician practices, of 1 to 100 employees. The data shows it takes a healthcare organization an average of 84 days to identify a breach, and 68 days to issue a notification of it. About half of the respondents in the Ponemon survey said their data breaches led to actual medical identify theft among their patients.
Source: http://www.darkreading.com/risk-management/167901115/security/attacks-breaches/240144006/most-healthcare-organizations-suffered-data-breaches.html

[Return to top]

Government Facilities Sector

17. *December 7, WBNG 12 Binghamton* – (Pennsylvania) **Courthouse evacuates after bomb threats.** The Bradford County Courthouse in Towanda, Pennsylvania, was evacuated after receiving bomb threats December 6. According to Pennsylvania State Police, the courthouse received two suspicious phone calls. The caller said that bombs were inside the courthouse. The Bradford County Sheriff's Department evacuated the courthouse. Six hours later, the Bomb Squad K-9 detection team cleared the scene. After an investigation, police said that a man from Rome, Pennsylvania, made the calls and threats. He had a sentencing hearing for a DUI charge December 6. He told police he made the threats because he wanted to spend the next couple of weeks with his family and not in jail. He was held in a county jail.
Source: http://www.wbng.com/news/local/Courthouse-Evacuates-After-Bomb-Threats-182489651.html

18. *December 7, Associated Press* – (Georgia) **Students back in school evacuated four days ago because of carbon monoxide.** Finch Elementary School in Atlanta reopened

December 7, 4 days after soaring levels of carbon monoxide sent more than 40 students and some adults to hospitals. School officials said carbon monoxide detectors were installed. Georgia law does not require the detectors in schools, but Atlanta Public Schools officials said December 6 that planning is under way to install them in buildings across the district. The school's superintendent said the leak was caused by human error, not an equipment failure. He said two maintenance workers serviced the boiler at the school just days before the leak, and failed to reopen a valve after doing the work.
Source: http://jacksonville.com/news/georgia/2012-12-07/story/students-back-school-evacuated-four-days-ago-because-carbon-monoxide

19. *December 6, Military Times* – (Virginia) **FBI: Retired sailor faces spy charges.** A former U.S. Navy sailor who served as a cryptologic technician was indicted by a federal grand jury for attempted espionage related to submarine tracking secrets. He was arrested December 6 in Virginia Beach, Virginia. According to the indictment, he attempted to deliver classified documents to someone he believed was a representative of the Russian Federation. The indictment says he actually delivered the information to the FBI, which was conducting an undercover operation. He served in the Navy for 20 years before he retired in November 2011. The indictment says he attempted to deliver the classified information in late October of 2011.
Source: http://www.militarytimes.com/news/2012/12/ap-former-sailor-arrested-espionage-120612/

[Return to top]

Emergency Services Sector

20. *December 7, Portland Press Herald* – (Maine) **Severed cable disables Windham 911.** A severed fiber optic cable left land lines in the Windham, Maine area unable to connect to 9-1-1, and people with emergencies were being urged to use cell phones instead. An alert from the Cumberland County Regional Communications Center December 7 said people in the 892 and 894 exchanges were affected. The dispatch center asked that they use a cell phone, their own or a neighbor's, to call 9-1-1 for emergencies. Crews were working on the line and planned on having it repaired by December 7.
Source: http://www.pressherald.com/news/maine-Windham-911-temporarily-disabled.html

21. *December 6, Lake County Record-Bee* – (California) **Clearlake fire personnel report equipment stolen.** Firefighters with California's Lake County Fire Protection District (LCFPD) discovered 40 gallons of gasoline were gone from the fire engine they were going to use for an emergency call November 25. Sometime between November 23 and November 25, someone broke into their airport property fire station, the chief said. He said robbers broke into the station and stole thousands of dollars worth of specialized equipment. This marked the second time in 2012 the LCFPD was robbed, and the losses totaled more than $13,000, the chief said. Currently, there are no leads as to who committed the robberies, and there is no evidence that the two are linked. Among items

stolen during the two instances were a medical bag, self-contained breathing apparatus (SCBA) masks, a chainsaw, and a box of beryllium tools worth $6,000, the chief said. He also said while four SCBA masks were stolen, the packets to properly use them were not therefore, they serve no function. Two axes priced at $1,000 from a 1947 American LaFrance fire engine were also taken.
Source: http://www.record-bee.com/ci_22141140/clearlake-fire-personnel-report-equipment-stolen?source=most_emailed

For another story, see item **29**

[Return to top]

Information Technology Sector

22. *December 7, IDG News Service* – (International) **Tor network used to command Skynet botnet.** Security researchers have identified a botnet controlled by its creators over the Tor anonymity network. It is likely that other botnet operators will adopt this approach, according to the team from vulnerability assessment and penetration testing firm Rapid7. The botnet is called Skynet and can be used to launch distributed denial-of-service (DDoS) attacks, generate Bitcoins — a type of virtual currency — using the processing power of graphics cards installed in infected computers, download and execute arbitrary files, or steal login credentials for Web sites, including online banking ones. However, what really makes this botnet stand out is that its command and control (C&C) servers are only accessible from within the Tor anonymity network using the Tor Hidden Service protocol. Tor Hidden Services are perfect for a botnet operation, said a security researcher at Rapid7 in an email December 7. "As far as I understand, there is no technical way neither to trace and definitely neither to take down the Hidden Services used for C&C." The researcher published a blog post about the Skynet botnet December 6. He believes that the botnet is the same one described by a self-confessed botnet operator in a "IAmA" (I am a) thread on Reddit seven months ago. Despite the wealth of information about the botnet offered by its creator on Reddit seven months ago, the botnet is still alive and strong. In fact, Rapid7 researchers estimate that the botnet's current size is of 12,000 to 15,000 compromised computers, up to 50 percent more than what its operator estimated 7 months ago.
Source: http://www.itworld.com/security/326374/tor-network-used-command-skynet-botnet

23. *December 7, Softpedia* – (International) **BlackHole exploit kit has difficulties in infecting Chrome users, experts say.** The notorious Blackhole exploit kit has difficulties when its victims utilize Google's Chrome Web browser. According to experts from Blue Coat, when potential victims are tricked into clicking on links that point to Blackhole-infested Web sites, they are presented with a "loading" or a "please wait" message, while in the background they are redirected to the exploit pages that infect their computers with a piece of malware. However, this only happens if the victim uses browsers such as Internet Explorer or Firefox. During the attack, when users are redirected to the exploit pages, a script checks the user agent to identify which browser is utilized. If Chrome is detected, the victims are not redirected to the

Blackhole page. Instead, they are taken to another malicious page where they are urged to install a rogue Chrome update. This happens because Blackhole uses vulnerabilities in popular applications – such as Adobe Reader, Java, and the browser itself – to push malware onto the victim's device. However, since Chrome renders PDF files by using its built-in reader, and it asks users for permission before running a Java applet, Blackhole cannot succeed in its malicious task.
Source: http://news.softpedia.com/news/BlackHole-Exploit-Kit-Has-Difficulties-in-Infecting-Chrome-Users-Experts-Say-312810.shtml

24. *December 7, Softpedia* – (International) **Necurs malware infects over 83,000 machines in November 2012, Microsoft says.** According to experts from Microsoft's Malware Protection Center, the Necurs malware has been spotted on 83,427 unique computers in November alone. Researchers reveal the fact that Necurs is usually distributed via Web sites that host the BlackHole exploit kit. Once the threat finds itself on a computer, it downloads additional malicious elements, disables security applications, and hides its components. Furthermore, the malware also allows its controllers to gain complete control over the infected device through its backdoor functionality. It can also send spam and install pieces of scareware. Experts reveal that the malware might even be capable of disabling Microsoft Security Essentials' real time protection. Microsoft researchers have published a technical analysis of how Necurs manages to accomplish all these tasks.
Source: http://news.softpedia.com/news/Necurs-Malware-Infects-Over-83-000-Machines-in-November-2012-Microsoft-Says-312884.shtml

25. *December 7, The Register* – (International) **Rare critical Word vuln is the star of December Patch Tuesday.** Microsoft is planning to release seven bulletins December 11, five of which tackle critical vulnerabilities, as part of its final Patch Tuesday update of 2012. All currently supported operating systems (including Windows 8 and Windows RT) will need patching. The updates feature critical updates for Internet Explorer (IE) 9 and IE 10 browser software, a critical update for Microsoft Word, and critical updates for some of Microsoft's server products (Exchange and Sharepoint). Qualys's chief technology officer singled out the Word update for particular attention. "Bulletin 3 is special, as it affects Microsoft Word and is rated critical, which happens very rarely," he said.
Source: http://www.theregister.co.uk/2012/12/07/patch_tuesday_dec_2012_pre_alert/

26. *December 7, Associated Press* – (International) **Hackers said to hit UN telecoms talks in Dubai.** Organizers of a U.N. conference on global telecommunications said December 6 that hackers apparently blocked their Web site and disrupted the talks. The U.N.'s International Telecommunications Union said the Web site was hit December 5, blocking access to its main page and interfering with a closed-door working group. It says it is still investigating but initial signs pointed to hackers. The statement says Internet traffic was diverted to a backup Web site for 2 hours before normal operations resumed.
Source: http://www.ctpost.com/business/technology/article/Hackers-said-to-hit-UN-telecoms-talks-in-Dubai-4096444.php

For more stories, see items **3** and **5**

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

27. *December 7, Lihue Garden Island* – (Hawaii) **Storm knocks KUAI 720AM off the air.** A Kaua'i, Hawaii country radio station was knocked off the air in a December 4 electrical storm. KUAI 720 AM Eleele has been off the air since December 4 when both the power and telephone communication systems were impacted by the storm, the chief engineer and operation manager for the KQNG radio group said. The Kaua'i Island Utilities Cooperative was able to restore power to the antenna and transmission tower. The chief engineer and operation manager said Hawaiian Telcom was hoping to reach the tower December 7, but their crews were experiencing a heavier repair load than usual from the storm on the west side of the island. Both the power and telephone systems need to be operational before he can assess if there was any damage to the equipment at the studio. There was no estimated time as to how long it will be before the station is back on the air.
Source: http://thegardenisland.com/news/local/storm-knocks-kuai-am-off-the-air/article_8f779414-4045-11e2-a753-0019bb2963f4.html

28. *December 7, New York Post* – (New York) **Mayor wants to have telecommunications services restored to Lower Manhattan by end of year.** Speaking December 7 at a forum on New York City's future after Hurricane Sandy, the city's mayor disclosed that he had a "long conversation" December 6 with the Verizon CEO and together they developed a plan to provide temporary telecommunications services to downtown buildings by the end of 2012. Verizon lost 95 percent of its copper wiring to the salt waters that enveloped its downtown system during the storm. The deputy mayor said Verizon has undertaken a monumental recovery effort and is replacing its unusable copper wires with advanced fiber optics. He said the company, with the city's help, will also work to provide interim service to the affected buildings.
Source:
http://www.nypost.com/p/news/local/mayor_bloomberg_sandy_weather_working_kH8q04Sqs6FGoxV7M5dUeJ

29. *December 6, CNET* – (National) **FCC fast tracks text-to-911 service.** The Federal Communications Commission (FCC) chairman announced December 6 that the four largest wireless carriers in the U.S. have agreed to fast track a service that will let people text the emergency 9-1-1 line. AT&T, Verizon Wireless, Sprint, and T-Mobile have all signed on and major deployments are planned to roll out in 2013. The service

should be fully available nationwide by May 15, 2014. Dubbed "Next Generation 9-1-1," the FCC has been working on this project for the last two years. The goal of the service is to offer people more ways to contact emergency officials, as well as improve the network to ensure it holds up for new communication technologies. According to the FCC chairman, a key component in Next Generation 9-1-1 is the rapid deployment of text messaging, photo, and video support. While the service is getting phased-in, the mobile carries will send an automatic "bounce back" text message when any attempts to reach 9-1-1 via text message fail. This bounce back message would come before the text-to-9-1-1 service is available in a certain area.
Source: http://news.cnet.com/8301-1023_3-57557711-93/fcc-fast-tracks-text-to-911-service/

30. *December 6, Visalia Times-Delta* – (California) **Visalia classic rock station knocked off air.** KIOO 99.7 FM Porterville was knocked off the air when a delivery truck hit and destroyed its broadcast tower on Lewis Hill in California, Visalia Times-Delta reported December 6. There were no injuries as a result of the accident but the antenna was so badly damaged it had to be removed. Momentum Broadcasting, the Visalia-based owners of the station, were trying to get a limited signal going, but a new tower will have to be erected, which may take up to two days, station management said.
Source: http://blogs.visaliatimesdelta.com/choices/2012/12/06/visalia-classic-rock-station-knocked-off-air/

For another story, see item **26**

[Return to top]

Commercial Facilities Sector

31. *December 7, Beverly Salem News* – (Massachusetts) **Massachusetts hotel fire sends motel guests fleeing.** A three-alarm fire broke out at Beverly Garden Suites in north Beverly, Massachusetts, December 6. Fire officials said nobody was hurt in the blaze, which drew dozens of firefighters from surrounding communities. The Beverly fire chief said the fire started in a first-floor suite of the two-story motel and was most likely caused by plumbers using a torch to fix a pipe. The workers had moved on to the next suite by the time the fire started. The fire traveled up the wall into the unit above. The motel's officer manager said some of the rooms were under 2 feet of water from the fire hoses. The fire chief said nobody would be able to stay at the motel December 6.
Source: http://www.firehouse.com/news/10839306/massachusetts-hotel-fire-sends-motel-guests-fleeing

32. *December 6, WAFF 48 Huntsville* – (Alabama) **Bomb squad called to Huntsville apartment complex.** Huntsville Fire Department, HEMSI, and Huntsville, Alabama Police responded to the scene of a possible pipe bomb at Imperial Gardens Apartments, WAFF 48 Huntsville reported December 6. Tenants were evacuated from the apartments and the entire parking lot was blocked off for more than two hours while authorities were looking for pipe bombs. Police said the complex's maintenance crew

was cleaning out a recently vacated unit when they uncovered two explosive devices in a back bedroom closet. The bomb squad detonated the devices without any problems. Huntsville police and the FBI are now trying to locate the previous renters.
Source: http://www.waff.com/story/20282721/bomb-squad-on-scene-at-huntsville-apartment-complex

[Return to top]

National Monuments and Icons Sector

33. *December 6, Associated Press* – (National) **Federal agencies pledge to improve protection of Native American sacred sites.** Protection of, and improving tribal access to, sites on federal land held sacred by American Indians and Alaska Natives will be bolstered under a memorandum of understanding signed December 6 by the U.S. Department of Agriculture, U.S. Department of Defense, U.S. Department of Energy, U.S. Department of the Interior, and the Advisory Council on Historic Preservation. The agreement comes just weeks after thieves made off with rock carvings from a sacred site in California's Sierra Nevada. The site on the Volcanic Tableland north of Bishop, California, was what land managers called one of the most significant rock art sites in the region. The agencies plan to work during the next five years to raise awareness about sacred sites by developing a Web site, a training program for federal employees, and guidance for managing sacred sites. Officials at the U.S. Department of Agriculture and the U.S. Forest Service also released a report which provides a list of recommendations for working more closely with tribes in the protection, interpretation, and access to such sites.
Source: http://www.washingtonpost.com/politics/federal-agencies-pledge-to-improve-protection-of-native-american-sacred-sites/2012/12/06/4d0207d6-3fe6-11e2-8a5c-473797be602c_story.html

[Return to top]

Dams Sector

Nothing to report

[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