Daily Open Source Infrastructure Report
20 May 2016

Top Stories

- Federal regulators released a final ruling May 18 prohibiting passengers and crewmembers from carrying battery-powered portable electronic smoking devices in checked baggage, and from charging the devices on board an aircraft. – *U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration* (See item **11**)
- An 80-foot stretch of bank along the Bloomfield Irrigation District Ditch in Farmington collapsed May 16, shutting off access to the ditch and prompting officials to declare a state of emergency, among other actions. – *Farmington Daily Times* (See item **14**)
- Officials reported May 18 that an additional 117 million LinkedIn users' emails and passwords were compromised as attackers were discovered selling the information on the Dark Web May 16 in relation to a 2012 breach. – *PC Magazine* (See item **23**)
- Noodles & Company officials reported May 16 that they were investigating a potential breach in its point-of-sales (PoS) systems after receiving reports of unusual transactions on customers' credit cards starting in January 2016. – *Krebs on Security* (See item **24**)

Fast Jump Menu

Energy Sector

Nothing to report

Chemical Industry Sector

1. *May 18, Asbury Park Press* – (New Jersey) **Chemical spill reported in Lakewood.** A May 18 chemical spill at Church & Dwight Company in Lakewood, New Jersey, prompted about 200 employees to be sent home and prompted HAZMAT crews to respond to the incident after a cloud or plume formed in the area following the spill. Officials are investigating the incident.
   Source: http://www.app.com/story/news/local/emergencies/2016/05/18/chemical-spill-lakewood/84554992/

Nuclear Reactors, Materials, and Waste Sector

2. *May 18, London Platts* – (Connecticut) **Dominion's Millstone 3 nuclear unit in Connecticut returns after hydrogen leak.** The U.S. Nuclear Regulatory Commission reported May 18 that Millstone Nuclear Power Plant's Unit 3 nuclear reactor in Waterford, Connecticut, was back online with limited capacity after the unit was shut down due to a main generator hydrogen gas leak into the turbine building. The source of the leak was identified and repaired and officials were unsure when the unit would resume full capability.
   Source: http://www.platts.com/latest-news/electric-power/washington/dominions-millstone-3-nuclear-unit-in-connecticut-21486429

3. *May 18, Associated Press; Idaho Falls Post Register* – (Idaho) **Nuclear-plant contractor fined for 2015 electrical explosion.** The U.S. Department of Energy fined Battelle Energy Alliance LLC $60,000 and reported that the company had deficiencies in their electrical safety program, protective equipment selection process, and hazard identification and assessment procedure, among other deficiencies, following an April 2015 incident where three Battelle workers were knocked down due to a preventable electrical explosion. Battelle officials stated they have implemented several safety procedures to mitigate future incidences.
   Source: http://www.ksl.com/index.php?nid=151&sid=39821330&title=nuclear-plant-contractor-fined-for-2015-electrical-explosion

Critical Manufacturing Sector

4. *May 18, Associated Press* – (Texas) **Toyota plant in Texas halts production due to storm damage.** The Toyota Motor Corp., assembly plant in San Antonio, Texas, suspended production May 18 until further notice following severe storms that caused a portion of the facility's roof to collapse and power outages throughout the facility due to water leaks.
   Source: http://abcnews.go.com/US/wireStory/parts-south-texas-hail-heavy-rain-flooding-39193455

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *May 18, San Diego Union-Tribune* – (California) **'Hipster Bandit' robs bank minutes after failed attempt.** Authorities are searching for a man dubbed the "Hipster Bandit" who is suspected of robbing a Union Bank branch and attempting to rob a Wells Fargo Bank branch in Oceanside, California, May 18. The man is suspected of robbing at least four other banks in San Diego County since July 2015.
Source: http://www.sandiegouniontribune.com/news/2016/may/18/hipster-bandit-robs-bank-oceanside/

6. *May 18, Fort Myers News-Press* – (Florida) **Naples men pleads guilty to defrauding insurance companies.** A Naples man pleaded guilty May 18 to Federal charges after the man and co-conspirators ran five unlicensed chiropractic clinics that received over $2 million in fraudulent insurance payments from car insurance companies by soliciting people to participate in staged vehicle accidents in exchange for compensation, and coaching the patients involved in the scheme to receive unneeded treatment. Officials stated the group used a shell corporation to conceal the proceeds from the fraudulent insurance claims and four other people were charged for their roles in the scheme.
Source: http://www.news-press.com/story/news/crime/2016/05/18/naples-men-pleads-guilty-defrauding-insurance-companies/84566156/

7. *May 17, SecurityWeek* – (International) **ATMs targeted with improved "Skimer" malware.** Researchers at Kaspersky Lab discovered a new version of an ATM malware dubbed, "Skimer" that allows attackers direct interaction with ATMs by inserting two types of cards with specially crafted Track 2 data into the infected machine; one designed to execute commands hardcoded in Track 2, while the other allows attackers to launch 1 of 21 predefined commands using the personal identification number (PIN) and malware interface to dispense money from the machine, collect the details of cards inserted, and print the information collected from cards. Researchers stated attackers can use the malware interface to delete the malware, debug it, and update it with code stored on the special card.
Source: http://www.securityweek.com/atms-targeted-improved-skimer-malware

Transportation Systems Sector

8. *May 19, South Jersey Courier-Post* – (New Jersey) **Medford crash sends five to hospitals.** A 3-vehicle crash prompted a nearly 5-hour closure of Route 70 in Medford, New Jersey, May 18 and sent five people to an area hospital with injuries.
Source: http://www.courierpostonline.com/story/news/2016/05/19/medford-crash-highway-closed/84577194/

9. *May 19, Greensburg Daily News* – (Indiana) **Early morning tanker spill shuts down SR 3.** A portion of State Road 3 in Greensburg, Indiana was closed for nearly 6 hours

May 18 after a semi-truck carrying approximately 7,500 gallons of ethanol overturned into a ditch, causing a small amount of fuel to spill. Crews cleaned up the spill after the semi-truck was removed.
Source: http://www.greensburgdailynews.com/news/local_news/early-morning-tanker-spill-shuts-down-sr/article_0775687a-1a62-52e3-818b-37ddf7597399.html

10. *May 18, Ventura County Star* – (California) **Man killed in head-on crash on Highway 118 in Moorpark.** Westbound lanes of Highway 118 in Ventura County were shut down for more than 2 hours May 18 after one driver was killed in a fatal head-on collision involving a semi-truck and another vehicle.
Source: http://www.vcstar.com/news/local/moorpark/fatal-crash-reported-on-highway-118-in-moorpark-331e4b8c-1104-60c4-e053-0100007f3858-379950261.html

11. *May 18, U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration* – (National) **DOT bans e-cigarettes from checked baggage.** The Pipeline and Hazardous Materials Safety Administration announced a final ruling May 18 prohibiting passengers and crewmembers from carrying battery-powered portable electronic smoking devices such as e-cigarettes, e-cigs, personal vaporizers, and other electronic nicotine delivery systems in checked baggage, and prohibiting passenger or crewmembers from charging the devices on board an aircraft. Passengers are allowed to carry the electronic smoking devices in carry-on baggage or on their person, but may not use them on flights.
Source: http://www.phmsa.dot.gov/hazmat/dot-bans-ecigarettes-from-checked-baggage

Food and Agriculture Sector

12. *May 19, U.S. Department of Agriculture* – (National) **Recall notification report 041-2016 (pork dumpling products).** Aurnish Enterprises Corporation issued a recall May 18 for approximately 5,616 pounds of its Aurnish Enterprise Corp. Pork Dumpling products sold in 1.25-pound packages due to misbranding and undeclared monosodium glutamate (MSG) discovered during a comprehensive Federal Food Safety Assessment (FSA) at the Woodside, New York facility. There have been no confirmed reports of adverse reactions and the products were distributed to institutional and retail locations in six States.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/rnr-041-2016

13. *May 18, U.S. Department of Labor* – (Wisconsin) **OSHA finds safety failures allowed machine to sever 30-year-old worker's three fingertips at Nature's Path subsidiary in Wisconsin.** The Occupational Safety and Health Administration cited Nature's Path USA II LLC with 2 repeated, 14 serious, and 1 other-than-serious safety violation May 17 following a November 2015 incident where a rotating airlock blade severed a worker's fingers while he cleaned the machine, prompting an investigation at the Sussex, Wisconsin facility, which revealed the company failed to power down or lock equipment to prevent unintentional operation, failed to install adequate machine guarding, and failed to train workers about chemical hazards, among other violations. Proposed penalties total $118,320.

Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32082

Water and Wastewater Systems Sector

14. *May 16, Farmington Daily Times* – (New Mexico) **Ditch breach cuts off Bloomfield's water supply.** An 80-foot stretch of bank along the Bloomfield Irrigation District Ditch in Farmington collapsed May 16 shutting off access to the ditch, prompting San Juan County officials to declare a state of emergency, discontinue watering parks and sports fields, urge residents to conserve water, and initiate repairs which are expected to take at least 2 weeks.
Source: http://www.daily-times.com/story/news/local/bloomfield/2016/05/16/ditch-breach-cuts-off-bloomfields-water-supply/84458332/

Healthcare and Public Health Sector

15. *May 18, WBIR 10 Knoxville* – (Tennessee) **TBI: Maynardville medical clinic owner busted in prescription drug fraud case.** The owner and operator of the Quality Medical Center in Union County, Tennessee, was arrested and charged May 18 for allegedly using patient identifying information to fraudulently obtain prescription medication for the benefit of others.
Source: http://www.wbir.com/news/local/claiborne-hancock-grainger-union/tbi-maynardville-medical-clinic-owner-busted-in-prescription-drug-fraud-case/202462098

Government Facilities Sector

16. *May 19, WLOS 13 Asheville* – (North Carolina) **3 teens arrested after two bomb threats reported at Madison High School.** Three students were arrested in connection to several bomb threats that prompted the closure of Madison High School in Madison County, North Carolina, May 19.
Source: http://wlos.com/news/local/authorities-on-scene-after-multiple-threats-reported-at-madison-high-school

Emergency Services Sector

17. *May 18, KWTX 10 Waco* – (Texas) **Teenager overpowers guard to escape local juvenile detention center.** Killeen police are searching for a teenager who overpowered a detention officer, stole keys to open the door, and fled from the Bell County Juvenile Detention Center May 18.
Source: http://www.kwtx.com/content/news/Teenager-escapes-from-local-juvenile-detention-center-379982561.html

18. *May 16, WJAC 6 Johnstown* – (Pennsylvania) **4 firefighters charged with submitting false reports to 911.** Logan Township police announced May 16 that four volunteer firefighters from the Logan Township United Fire Department's Kittanning Trail Station were charged with allegedly calling 9-1-1 on several occasions between January

and March to report false fires in order to ride in a fire truck.
Source: http://wjactv.com/news/local/4-firefighters-charged-with-submitting-false-reports-to-911

Information Technology Sector

19. *May 19, Softpedia* – (International) **A quarter of all hacked WordPress sites can be attributed to three plugins.** Sucuri conducted an investigation on over 11,485 compromised Web sites and released its "Website Hacked Report" which revealed that during the first 3 months of 2016, 78 percent of hacked Web sites were using the WordPress Content Management System (CMS) platform and found that attackers were primarily using outdated plugins to hack WordPress sites. Outdated plugins included RevSlider, GravityForms, and TimThumb, but officials concluded that only 56 percent of all WordPress sites were running outdated WordPress core versions.
Source: http://news.softpedia.com/news/a-quarter-of-all-hacked-wordpress-sites-can-be-attributed-to-three-plugins-504240.shtml

20. *May 19, Softpedia* – (International) **TeslaCrypt ransomware project appears to shut down, offers free decryption key.** Security researchers from ESET found that the TeslaCrypt ransomware operation will be shut down and the operators of the ransomware agreed to offer a master decryption key for all victims infected with the TeslaCrupt v3 and v4 after a researcher contacted the ransomware operator using the ransom Web site hosted on the Dark Web via their support channel.
Source: http://news.softpedia.com/news/teslacrypt-ransomware-project-appears-to-shut-down-offers-free-decryption-key-504234.shtml

21. *May 18, Agence France-Presse* – (International) **Cyber attackers target US presidential campaigns: Official.** The DHS and the FBI are investigating cyberattacks against the campaigns of the U.S. presidential candidates after the director of the U.S. National Intelligence Council reported there were indications that revealed cyber attackers were targeting both the Democratic and Republican representatives. Officials stated the attacks could range from defacement to intrusion.
Source: http://www.securityweek.com/cyber-attackers-target-us-presidential-campaigns-official

22. *May 18, SecurityWeek* – (International) **Macro malware makes improvements on hiding malicious code.** Security researchers from Microsoft's Malware Protection Center discovered a new variation of the Donoff macro malware had evolved to avoid detection after finding that the malware was disseminated via spam email campaigns with attachments made to look non-malicious. The attachments contain seven Visual Basic for Applications (VBA) modules with an encrypted string in the Caption field for CommandButton3 and an unusual code in Module2.
Source: http://www.securityweek.com/macro-malware-makes-improvements-hiding-malicious-code

23. *May 18, PC Magazine* – (International) **117M LinkedIn passwords leaked.** LinkedIn officials reported May 18 that an additional 117 million LinkedIn users' emails and

passwords were compromised as attackers were discovered selling the information on the Dark Web May 16 following a 2012 breach where a hacker named "Peace" gained unauthorized access and compromised more than 6 million users' accounts. The social network reported that the additional compromised accounts were not a result of a new security breach and were working to apply a password reset to potentially compromised accounts.
Source: http://www.pcmag.com/news/344568/117m-linkedin-passwords-leaked

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: http://www.it-isac.org

Communications Sector

Nothing to report

Commercial Facilities Sector

24. *May 19, Krebs on Security* – (National) **Noodles & Company probes breach claims.** Noodles & Company officials reported May 16 that they were investigating a potential breach in its point-of-sales (PoS) systems after receiving reports from financial institutions who detected unusual transactions on customers' credit cards at various restaurant locations starting in January 2016.
Source: http://krebsonsecurity.com/2016/05/noodles-company-probes-breach-claims/

25. *May 18, WFAA 8 Dallas* – (Texas) **Red Cross assisting after 3-alarm apartment fire in Grapevine.** A 3-alarm fire May 18 at the Ridge Crest Apartments in Grapevine, Texas, damaged up to 18 apartment units and prompted a building evacuation due to a cooking fire. No injuries were reported and firefighters contained the incident.
Source: http://www.wfaa.com/news/local/tarrant-county/red-cross-assisting-after-3-alarm-apartment-fire-in-grapevine/201843075

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 cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
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