



## Daily Open Source Infrastructure Report 29 March 2016

### Top Stories

- The Kyle Public Works Department worked to contain a spill of more than 117,000 gallons of wastewater that reached the Bunton Branch in Texas March 25 after storms reportedly caused pumps to fail when power was knocked out. – *KXAN 36 Austin* (See item [9](#))
- Officials reported March 25 that the personal information of more than 3,000 employees at Tidewater Community College in Virginia was leaked after an employee sent a file containing employees’ information in response to a data request from a fraudulent college account March 2. – *Norfolk Virginian-Pilot* (See item [15](#))
- A March 25 fire inside a recording studio at Boston University’s College of Communication caused about \$500,000 in damages and injured a university police officer, 3 students, and a firefighter. – *WCVB 5 Boston* (See item [16](#))
- Vormetric released its 2016 Data Threat Report which detailed that 90 percent of Information Technology (IT) security executives from large international organizations expressed their organizations were vulnerable to data threats. – *SecurityWeek* (See item [24](#))

---

### 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

Nothing to report

## Chemical Industry Sector

1. *March 28, U.S. Environmental Protection Agency* – (Pennsylvania) **EPA reaches settlement with Brenntag Northeast for alleged environmental violations at Reading, Pa. facility.** The U.S. Environmental Protection Agency reported March 28 that Brenntag Northeast, Inc., a chemical repackaging and distribution plant in Reading, Pennsylvania, agreed to pay \$55,000 in penalties and donate \$30,000 of emergency response equipment to a local fire department after the company allegedly violated Federal and State regulations concerning the storage of hazardous waste and oil by failing to adequately control emissions of volatile waste, failing to plan for oil spill prevention, and failing to conduct timely inspections, among other violations.

Source:

<https://yosemite.epa.gov/opa/admpress.nsf/0/b58ffd2a20ccf2d085257f84004e8337>

## 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. *March 25, U.S. Securities and Exchange Commission* – (New Jersey; California) **SEC halts fraud by manager of investments in pre-IPO companies.** The U.S. Securities and Exchange Commission (SEC) announced March 25 charges and asset freezes against a New Jersey-based fund manager and 2 share-marketing companies, Saddle River Advisors and SRA Management Associates, after they allegedly stole \$5.7 million from investors, diverted millions more to improper and undisclosed uses, failed to register the share offerings with the SEC, and concealed the illicit activity by avoiding outside reviews of the funds, indiscriminately transferring money to more than a dozen bank accounts, and failing to provide investors with financial statements. Officials stated that the manager raised more than \$53 million from investors through the 2 funds and used the money to pay off earlier investors, prop up other funds, and pay family-related expenses, thereby leaving his firms unable to buy shares promised to investors.

Source: <https://www.sec.gov/news/pressrelease/2016-57.html>

## Transportation Systems Sector

3. *March 28, Wantagh-Seaford Patch* – (New York) **Five hospitalized after Sunrise Highway crash.** Eastbound lanes of Sunrise Highway in Seaford, New York, were closed for approximately 2 hours March 28 following an accident that left 5 people injured.  
Source: <http://patch.com/new-york/wantagh/five-hospitalized-after-seaford-crash>
4. *March 25, Southern California City News Service* – (California) **Big rig driver injured, 1 killed in Ortega Highway collision.** A crash involving a semi-truck and another vehicle shut down Ortega Highway between Avenida Siega and Antonio Parkway in Orange County for several hours March 25 while crews worked to clear the wreckage.  
Source: <http://mynews1a.com/orange-county/2016/03/25/big-rig-driver-injured-1-killed-in-ortega-highway-collision/>
5. *March 25, WRC 4 Washington, D.C.* – (Virginia) **Regular Metro service resumes after tunnel fire near Clarendon Station.** Orange and Silver line service on the Metrorail was halted for about 3 hours March 25 due to a fire between the Clarendon and Courthouse stations in Virginia. Authorities believe that the fire was electrical and likely caused by burning debris on the track bed.  
Source: <http://www.nbcwashington.com/news/local/Metro-Service-Suspended-Between-Rosslyn-Ballston-373545071.html>

## Food and Agriculture Sector

6. *March 26, U.S. Food and Drug Administration* – (National) **Smallbatch Pets Inc. voluntarily recalls frozen dog Duckbatch Sliders due to possible Salmonella and Listeria monocytogenes health risk.** Smallbatch Pets Inc., issued a voluntary recall March 26 for 1 lot of its frozen dog Duckbatch Sliders products sold in 3-pound packages after routine testing revealed the presence of Salmonella and Listeria monocytogenes in the products, which can pose a risk to humans handling the contaminated products. No illnesses have been reported and the products were distributed to retail locations in California, Colorado, Oregon, and Washington.  
Source: <http://www.fda.gov/Safety/Recalls/ucm492628.htm>
7. *March 25, Food Safety News* – (Minnesota; Wisconsin) **CDC declares end to E.coli outbreak linked to fresh sprouts.** The U.S. Centers for Disease Control and Prevention announced March 25 that the E.coli outbreak linked to Jack & The Green Sprouts, Inc., alfalfa sprouts products has ended. The outbreak sickened 11 people in Minnesota and Wisconsin from January 17 – February 17.  
Source: <http://www.foodsafetynews.com/2016/03/cdc-declares-end-to-e-coli-outbreak-linked-to-fresh-sprouts/#.VvkdtIrKUK>
8. *March 25, U.S. Food and Drug Administration* – (National) **Trader Joe's issues voluntary allergy alert on undeclared milk in Chocolate Orange Sticks and Chocolate Raspberry Sticks.** Trader Joe's issued a voluntary recall March 25 for all

lots of its Chocolate Orange Sticks products and Chocolate Raspberry Sticks products sold in 18-ounce packages due to mislabeling and undeclared milk allergens after the company noticed discoloration in the product's coating. Two allergic reactions have been reported and the products were distributed to Trader Joe's stores nationwide.  
Source: <http://www.fda.gov/Safety/Recalls/ucm492617.htm>

## Water and Wastewater Systems Sector

9. *March 26, KXAN 36 Austin* – (Texas) **More than 117,000 gallons of wastewater spills in Kyle.** The Kyle Public Works Department worked to contain a spill of more than 117,000 gallons of wastewater that reached the Bunton Branch in Texas March 25 after storms reportedly caused pumps to fail when power was knocked out. Clean up is estimated to take 10 – 14 days while crews drain the creek and pump fresh water to dilute the remaining contaminants.  
Source: <http://kxan.com/2016/03/25/more-than-100000-gallons-of-wastewater-spills-in-kyle/>
10. *March 25, Charlotte Observer* – (North Carolina) **Broken pipe blamed for Charlotte sewage spill.** Charlotte Water reported that approximately 1,470 gallons of sewage entered Sugar Creek March 24 after a total of 2,940 gallons spilled due to a broken pipe near Granite Street.  
Source: <http://www.charlotteobserver.com/news/local/article68223902.html>

## Healthcare and Public Health Sector

11. *March 26, Associated Press* – (Alabama) **Helicopter crew, patient killed in southeast Alabama crash.** Three crew members and a patient were killed when a medical helicopter en route to Troy Regional Medical Center crashed in southeast Alabama March 26. Authorities are investigating the incident.  
Source: <http://www.foxnews.com/us/2016/03/26/helicopter-crew-patient-killed-in-southeast-alabama-crash.html>
12. *March 25, Iowa City Press-Citizen* – (Iowa) **Mercy Iowa City warns patients of privacy breach.** Mercy Iowa City and Mercy Clinics notified an undisclosed amount of patients March 25 that their personal, medical, and health insurance information may have been accessed after officers informed Mercy Hospital in Iowa of a computer virus that potentially infected some of its systems January 26. The health clinic worked to secure its systems and continues to investigate the incident.  
Source: <http://www.press-citizen.com/story/news/local/2016/03/25/mercy-iowa-city-privacy-breach/82271988/>

## Government Facilities Sector

13. *March 28, Battle Creek Enquirer* – (Michigan) **Police say no evidence Lakeview threat is credible.** School officials closed all Lakeview School District buildings in Battle Creek March 28 due to threats posted on a social media site claiming to detonate bombs and shoot students March 27. An investigation is ongoing after police

determined that the threats were not credible.

Source: <http://www.battlecreekenquirer.com/story/news/local/2016/03/28/bomb-threat-closes-lakeview-schools-today/82333708/>

14. *March 27, Wichita Eagle* – (Kansas) **Easter snowfall helps tame Barber County wildfire.** The Kansas Forest Service announced March 27 that a State wildfire that burned nearly 400,000 of acres was 90 percent contained. Crews worked to put out hot-spots and officials are assessing the total amount of damage.  
Source: <http://www.kansas.com/news/state/article68514047.html>
15. *March 25, Norfolk Virginian-Pilot* – (Virginia) **Data breach exposes information on more than 3,000 TCC employees.** Officials announced March 25 that personal information, including Social Security numbers, of more than 3,000 employees at Tidewater Community College (TCC) in Virginia was leaked when an employee sent a file March 2 that included personal information of employees in response to a data request from a fraudulent TCC email account.  
Source: [http://pilotonline.com/news/local/crime/data-breach-exposes-information-on-more-than-tcc-employees/article\\_6ab72a2f-52a0-533e-8060-a2d245c7f151.html](http://pilotonline.com/news/local/crime/data-breach-exposes-information-on-more-than-tcc-employees/article_6ab72a2f-52a0-533e-8060-a2d245c7f151.html)
16. *March 25, WCVB 5 Boston* – (Massachusetts) **5 suffer smoke inhalation in Boston University campus fire.** A March 25 fire inside a recording studio at Boston University's College of Communication caused about \$500,000 in damages and sent a university police officer, 3 students, and a firefighter to an area hospital for smoke inhalation. The building was evacuated and ventilated after investigators determined that the studio's sound insulation in the walls produced high levels of hydrogen cyanide.  
Source: <http://www.wcvb.com/news/fire-reported-on-boston-university-campus/38690464>
17. *March 25, Central Connecticut Town Times* – (Connecticut) **Hammonasset to receive nearly \$12 million for projects.** The Connecticut State Bond Commission approved nearly \$12 million in funding for projects in Madison March 25, including the replacement of electrical, water, and natural gas systems at Hammonasset Beach State Park.  
Source: <http://www.towntimes.com/news/allnews/8629700-129/hammonasset-to-receive-nearly-12-million-for-projects.html>

## Emergency Services Sector

18. *March 25, WCYB 5 Bristol* – (Tennessee) **Kingsport 911 center backup power glitch revealed, repaired.** Crews replaced faulty pieces in an insulator that caused 9-1-1 calls at the Kingsport Emergency Communications Center in Tennessee to be rerouted for several hours March 25. Computer, radio, and phone systems were temporarily shut down when the communications center did not automatically switch over to backup generator power.  
Source: <http://www.wcyb.com/news/power-outage-disrupts-911-center/38689856>

## Information Technology Sector

19. *March 28, SecurityWeek* – (International) **PowerWare ransomware abuses PowerShell, Office macros.** Security researchers from Carbon Black reported a new fileless ransomware, PowerWare can allow attackers to disguise malicious commands as legitimate computer activities and execute malicious actions by abusing PowerShell, a core utility for Microsoft Windows systems. The malware was distributed via malicious Word documents that uses embedded macros to send “cmd.exe” to a target’s computer.  
Source: <http://www.securityweek.com/powerware-ransomware-abuses-powershell-office-macros>
20. *March 28, Softpedia* – (International) **Flaw in StartSSL validation allowed attackers to get SSL certs for any domain.** A security researcher discovered a domain validation flaw in Web service, StartSSL certificate authority (CA) that could allow an attacker to receive Secure Sockets Layer (SSL) certificates for any desired domain by capturing the Hypertext Transfer Protocol (HTTP) request sent to the server and modifying the included parameters to send the certificate to their own personal email. StartSSL reported they patched the flaw.  
Source: <http://news.softpedia.com/news/flaw-in-startssl-validation-allowed-attackers-to-get-ssl-certs-for-any-domain-502257.shtml>
21. *March 27, Softpedia* – (International) **WordPress attacked 3.5 times more often than non-CMS sites.** Security firm, Imperva released a report stating that Web attacks in 2015 increased greatly after the company analyzed about 7 generic attacks and more than 24 million alerts for 200 Web applications, which revealed that Structured Query Language (SQL) injections tripled and cross-site scripting (XSS) attacks doubled within the year. In addition, the report found many attacks were in Web applications running on standard Content Management System (CMS) platforms, which were attacked three times more than non-CMSs applications, among other findings.  
Source: <http://news.softpedia.com/news/wordpress-attacked-3-5-times-more-than-non-cms-sites-502232.shtml>
22. *March 26, Softpedia* – (International) **Node.js Package Manager vulnerable to malicious worm packages.** A Google software engineer discovered that a design flaw in Node.js Package Manager (npm) could allow an attacker to infect other packages and propagate malicious scripts in the entire JavaScript ecosystem as well as in the structure of projects via a simple worm virus, which can be distributed through a rogue npm package embedded with malicious code. Once a malicious package is opened, unaware developers will include the package in projects via a “npm install” command, which will execute malicious actions on the infected system using the users’ full privileges.  
Source: <http://news.softpedia.com/news/node-js-package-manager-vulnerable-to-malicious-worm-packages-502216.shtml>
23. *March 25, SecurityWeek* – (International) **Google patches serious flaws in Chrome 49.** Google released patches for Chrome 49 affecting Microsoft Windows, Apple Mac,

and Linux systems that fixed five vulnerabilities including a use-after free vulnerability in Navigation and Extensions, an out-of-bounds read in V8 JavaScript engine, and a buffer overflow flaw in LibAGLE, among other flaws.

Source: <http://www.securityweek.com/google-patches-serious-flaws-chrome-49>

24. *March 25, SecurityWeek* – (International) **U.S. Federal Agencies vulnerable to data threats: Survey.** Vormetric released its 2016 Data Threat Report which detailed that 90 percent of Information Technology (IT) security executives from large international organizations, including more than 100 executives in the U.S. Federal government expressed their organizations were vulnerable to data threats and that 61 percent of executives admitted that their organization had previously suffered a data breach. The report stated that many entities were planning to increase spending on sensitive data protection, invest in data-at-rest defenses, and implement more efficient data security tools.

Source: <http://www.securityweek.com/us-federal-agencies-vulnerable-data-threats-survey>

25. *March 25, SecurityWeek* – (International) **Petya ransomware encrypts entire hard drives.** Security researchers from G DATA SecurityLabs found a new threat, dubbed Petya ransomware that has been allegedly encrypting company's entire hard drives and locking users out of their systems via a malicious Dropbox download link, included in an email sent to Human Resources (HR) departments, that is embedded with an executable file that causes the computer to crash and enables the ransomware to manipulate the Master Boot Record (MBR) to ultimately control the computer system. Security researchers advised HR department employees to take extra precaution when offered Dropbox links.

Source: <http://www.securityweek.com/petya-ransomware-encrypts-entire-hard-drives>

26. *March 25, SecurityWeek* – (International) **Brazilian trojan conceals malicious code in PNG image.** Security researchers from Kaspersky Lab found a new malware delivery method was being used by attackers to avoid detection after finding that attackers were distributing a Portable Network Graphics (PNG) image embedded with malicious code via an email that contains a clean PDF file, which holds a link to a .zip file with the malicious image. Researchers found that the PNG image cannot be executed without its launcher; and therefore, it cannot be the main infector.

Source: <http://www.securityweek.com/brazilian-trojan-conceals-malicious-code-png-image>

### 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

Nothing to report

## Commercial Facilities Sector

27. *March 28, Danbury News-Times* – (Connecticut) **40 people affected by Danbury apartment fire.** Officials reported March 28 that a fire at a Danbury building housing 24 apartments and several businesses displaced 30 residents after the blaze burned 2 apartment units. No injuries were reported and the cause of the incident is under investigation.  
Source: <http://www.newstimes.com/local/article/Fire-reported-at-four-story-building-in-Danbury-7209951.php>
28. *March 27, WVEC 13 Hampton* – (Virginia) **60 people displaced after Portsmouth apartment fire.** Approximately 60 residents from The Quarters apartment complex in Portsmouth, Virginia, were displaced March 26 after an improperly discarded cigarette, or other smoking material, caused a balcony fire. Fifteen apartment units were damaged and fire crews remained on site for about 2 hours containing the incident.  
Source: [http://www.13newsnow.com/news/local/mycity/portsmouth/60-people-displaced-after-portsmouth-apartment-fire\\_/103391493](http://www.13newsnow.com/news/local/mycity/portsmouth/60-people-displaced-after-portsmouth-apartment-fire_/103391493)

## 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.