

UNCLASSIFIED



NORTH DAKOTA

Critical Infrastructure and Key Resources (CI/KR) Ticker



The North Dakota Open Source (CI/KR) Ticker a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the (CI/KR) Ticker to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The (CI/KR) Ticker is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

TABLE OF CONTENTS

[North Dakota](#) 3

[Regional](#) 3

[National](#) 4

[International](#) 4

[Banking and Finance Industry](#) 5

[Chemical and Hazardous Materials Sector](#) 5

[Commercial Facilities](#) 5

[Communications Sector](#) 6

[Critical Manufacturing](#) 6

[Defense/ Industry Base Sector](#) 7

[Emergency Services](#) 7

[Energy](#) 7

[Food and Agriculture](#) 8

[Government Sector \(including Schools and Universities\)](#) 9

[Information Technology and Telecommunications](#) 9

[Public Health](#) 11

[Transportation](#) 12

[Water and Dams](#) 12

[North Dakota Homeland Security Contacts](#) 13

UNCLASSIFIED

NORTH DAKOTA

(North Dakota) Emergency warning system being beefed up in Williams County. Officials are installing outdoor warning sirens across Williams County and urging residents to sign up for phone- and computer-based alerts.

http://bismarcktribune.com/news/state-and-regional/emergency-warning-system-being-beefed-up-in-williams-county/article_0efe7540-3532-5bdf-849a-3d10edf02fc8.html

(North Dakota) Lightning strikes, burns saltwater disposal well site in Dunn County. A lightning strike Sunday at a saltwater disposal well about 4 miles southwest of Manning led to a "very large explosion," Dunn County Emergency Manager Denise Brew said, and burned 640 barrels of oil and 640 barrels of saltwater on Sunday.

<http://www.thedickinsonpress.com/energy/water/4017317-lightning-strikes-burns-saltwater-disposal-well-site-dunn-county>

(North Dakota) Fargo Country Club taking its flood protection to another level. The flood wall is taking FCC's war with the Red River to another level. At a cost of \$1.7 to \$1.8 million that will be paid by the membership, it's the first phase of what is hoped to be a three-phase project to deal with the potential of the rising Red. <http://www.inforum.com/sports/4012708-fargo-country-club-taking-its-flood-protection-another-level>

REGIONAL

(Wisconsin) Schools begins in Antigo, press conference at 2 p.m. The Antigo Police Department announced that a gunman was shot and killed by an officer after he shot and injured two students at random April 23 at Antigo High School as they left for prom. Classes at the high school resumed April 25 while the incident remains under investigation.

<http://www.wsaw.com/content/news/Breaking-News-Shooting-at-Antigo-High-School-Prom-376879681.html>

(Wyoming) Wyoming Medical Center informs 3,200 patients of email breach. Wyoming Medical Center in Casper notified 3,184 patients April 20 that their

UNCLASSIFIED

UNCLASSIFIED

personal and medical information may have been potentially exposed in a phishing scam that targeted 2 employees February 22. Medical center officials do not believe any of the information was misused, and stated that the access was immediately blocked upon discovery of the scheme.

http://trib.com/news/local/casper/wyoming-medical-center-informs-patients-of-email-breach/article_b88e758c-28fa-5470-9dd8-ad962f978b0d.html

NATIONAL

(National) Violence erupts in Seattle as May Day marchers face off with police. anti-capitalist protesters clashed with police in downtown Seattle on Sunday as May Day mayhem erupted again following a peaceful march. At least five officers had been injured and at least nine people had been arrested.

<http://www.chicagotribune.com/news/nationworld/ct-may-day-marches-violence-seattle-20160502-story.html>

INTERNATIONAL

(International) American Company Requests US to Ban China Steel Imports Due to Past Hacking. US Steel Corp, an American steel manufacturer, has filed a petition with the US government, asking it to intervene and ban all steel imports from Chinese companies. The steel maker is arguing that, in the past years, Chinese hackers have broken into the company's servers and stolen intellectual property regarding its manufacturing process.

<http://news.softpedia.com/news/american-company-requests-us-to-ban-china-steel-imports-due-to-past-hacking-503480.shtml#ixzz47WdlHkBA>

(International) Pentagon working to 'take out' Islamic State's internet. Pentagon officials reported April 28 that the U.S. military's Cyber Command (CYBERCOM) was working to destroy the Islamic State's Internet connection and leave the terrorist group in virtual isolation by interrupting the Islamic State's command and control (C&C), interrupting the group's ability to move funds, and interrupting the group's ability to recruit externally, among other actions. The task will be the command's first major combat operation in relation to the Islamic State threat.

UNCLASSIFIED

UNCLASSIFIED

<http://www.securityweek.com/pentagon-working-take-out-islamic-states-internet>

(International) Verizon 2016 DBIR: What you need to know. Verizon released its 2016 Data Breach Investigations Report (DBIR) which revealed current information technology (IT) trends and the overall cyberattack landscape after conducting an analysis on over 100,000 security incidents, which confirmed 2,260 data breaches occurred across 82 different countries in 2015, with the majority of breaches occurring due to human nature via phishing campaigns.

<http://www.securityweek.com/verizon-2016-dbir-what-you-need-know>

BANKING AND FINANCE INDUSTRY

Nothing Significant to Report

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

COMMERCIAL FACILITIES

(Maryland) Man in animal costume shot after making bomb threat at Baltimore's FOX45. The WBFF-TV news station building in Baltimore was evacuated for several hours April 28 after a man dressed in a panda "onesie" and armed with a fake vest bomb, allegedly threatened to blow up the building after being denied entry into the station's lobby when he insisted the news station air a story saved on a flash drive. Police crews, a SWAT team, and a bomb squad apprehended the man after shooting the suspect when he was non-compliant with officers. <http://foxbaltimore.com/news/local/fox45-evacuated-after-reported-threat-vehicle-fire>

(Connecticut) Employees stole almost \$300K of Home Depot merchandise: Police. Trumbull, Connecticut authorities issued arrest warrants April 22 for 7

UNCLASSIFIED

UNCLASSIFIED

Home Depot employees after the group allegedly stole approximately \$300,000 worth of merchandise following a store manager's report of missing power tools in October 2015. Police reviewed security camera footage and discovered that the group borrowed a store manager's key to steal products.

<http://www.nbcconnecticut.com/news/local/Trumbull-Home-Depot-Robbed-Blind-by-Store-Employees-Police-376801121.html>

COMMUNICATIONS SECTOR

(International) Android ransomware dropped via Towelroot, hacking team exploits. Security researchers from Blue Coat Labs discovered that a ransomware named "Cyber.Police" was able to install malicious programs onto a mobile device without user interaction after finding that at least 224 devices running Android versions 4.0.3 to 4.4.4 were communicating the malware's command and control (C&C) server since February and that the malicious programs were on devices running Cyanogenmod 10 version of Android 4.2.2. The malware was delivered via two known exploits including the Towelroot exploit and a JavaScript exploit.

<http://www.securityweek.com/android-ransomware-dropped-towelroot-hacking-team-exploits>

CRITICAL MANUFACTURING

(International) How Do You Stop 3D Printed Counterfeits? With 3D printing technologies emerging rapidly and a wide variety of industries looking to adopt 3D printing to streamline production and save on material costs, there is a lot of potential for market expansion and counterfeiting.

<http://www.ecnmag.com/article/2016/04/how-do-you-stop-3d-printed-counterfeits>

(International) 202,000 Ford vehicles recalled for transmission issue. The Ford Motor Company issued a recall April 27 for approximately 202,000 of its model years 2011 – 2012 F-150, and model year 2012 Expedition, Mustang, and Lincoln Navigator vehicles due to a malfunction in a speed sensor's software which can force the vehicle to unexpectedly downshift to first gear. The recall also includes

UNCLASSIFIED

UNCLASSIFIED

81,000 of Ford's model years 2014 –2015 Explorer vehicles sold in the U.S., Canada, and Mexico due to faulty rear suspension links that could fracture due to poor welds and have reportedly caused one accident and an injury.

<http://www.abcactionnews.com/news/national/202000-ford-vehicles-recalled-for-transmission-issue>

(International) GM to temporarily close 4 North American plants. General Motors Company announced April 22 that its assembly plants in Spring Hill, Tennessee; Lordstown, Ohio; Fairfax, Kansas; and a facility in Canada will be closed April 25 and remain idle for 2 weeks due to an electrical parts shortage following recent earthquakes in Japan.

<http://www.detroitnews.com/story/business/autos/general-motors/2016/04/22/gm-idling-four-plants/83386806/>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

(Texas) Van Zandt Co making backup plans after 911 blackout. Van Zandt County authorities announced April 25 that severed optic lines caused 9-1-1 service to go down for 10 hours April 23. The severed lines also cut Internet, landline, and cellular service for AT&T customers in the county.

<http://www.kxxv.com/story/31812513/van-zandt-co-making-backup-plans-after-911-blackout>

ENERGY

(Pennsylvania) State investigating quakes near Pa. fracking sites. The Pennsylvania Department of Environmental Protection announced April 27 that it is investigating the cause of a 1.9 earthquake April 25 in Lawrence County near a Hilcorp Energy Co., doing business as North Beaver NC Development site where the company was hydraulically fracturing two wells in a four-well pad in

UNCLASSIFIED

UNCLASSIFIED

Mahoning Township. State officials reported that the company stopped fracking operations and demobilized following the incident. <http://powersource.post-gazette.com/powersource/companies/2016/04/27/Pennsylvania-DEP-investigating-quakes-near-Hilcorp-Energy-fracking-shale-well-site-Lawrence-County/stories/201604270180>

(Virginia) Dominion Va. Power to start pouring treated coal ash water into James River on Wednesday. Dominion Virginia Power announced April 25 that it will use a 7-step cleaning process to ensure that water from Bremo Power Station's coal ash ponds do not harm the James River after the utility reached a settlement with the James River Association in March, which requires the company to clean the water to levels more stringent than State standards and to test fish tissue from the river. http://www.richmond.com/news/article_250fa66d-18c9-50a6-a5eb-94b6f574095a.html

(Michigan) BWL: Cyber attack didn't compromise customer info. Lansing Board of Water and Light announced April 25 that email, phones, computers, printers, and other technology on the corporate computer network remained shut down following a cyber-attack that utilized ransomware. The company asserted that customer and employee personal information was not compromised and that operations will continue. <http://www.lansingstatejournal.com/story/news/2016/04/25/police-investigate-cyber-attack-bwl/83500826/>

FOOD AND AGRICULTURE

(Michigan) Three indicted in alleged \$5 million food stamp fraud scheme. An indictment unsealed April 26 charged three people for their roles in an alleged food stamp fraud scheme that stole over \$5 million from Michigan State food stamp benefits and was run out of Shorthorn Meats and a nearby car wash in Flint from December 2011 - September 2014. The trio reportedly conspired to charge customers a commission for converting their Bridge Card food stamp benefits into cash by providing customers receipts of unpurchased food items that was turned over to a nearby car wash where customers obtained cash in the amount of roughly half of what was deducted from the Bridge Card by the suspects.

UNCLASSIFIED

UNCLASSIFIED

http://www.mlive.com/news/flint/index.ssf/2016/04/three_indicted_in_alleged_5_mi.html#incart_most-read_news_article

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Colorado; New Mexico; Utah) EPA paying \$1 million in response costs after mine spill. The U.S. Environmental Protection Agency announced April 28 that it will reimburse Colorado, New Mexico, and Utah State governments, the Navajo Nation, Southern Ute Indian Tribe, and Colorado counties and towns about \$1 million for costs attributed to an August 2015 wastewater spill that released 3 million gallons of water containing arsenic, cadmium, copper, lead, mercury, and other dangerous pollutants from the inactive Gold King Mine in Colorado.

<http://www.seattletimes.com/nation-world/epa-paying-1-million-in-response-costs-after-mine-spill/>

(Colorado) Student hospitalized after explosion in science room at Hidden Lake High School in Westminster. Students were evacuated and classes were cancelled at Hidden Lake High School in Westminster April 27 after a student was injured following a chemical reaction in a laboratory class. The building was ventilated and classes were expected to resume April 28.

<http://www.thedenverchannel.com/news/front-range/westminster/student-hospitalized-after-explosion-in-science-room-at-hidden-lake-high-school-in-westminster>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

(International) Law enforcement, government agencies see phishing as main cyber risk. The Global Cyber Alliance (GCA), a group of government representatives from the U.S. and the United Kingdom, agreed to promote the usage of Domain-based Message Authentication, Reporting & Conformance (DMARC) protocol to make it more difficult for attackers to tamper with original documents as phishing attacks were ranked as the top cyber threat following research that revealed spear-phishing campaigns increased by 55 percent from

UNCLASSIFIED

UNCLASSIFIED

2015. <http://news.softpedia.com/news/law-enforcement-government-agencies-see-phishing-as-main-cyber-risk-503272.shtml>

(International) Slack API credentials left in GitHub repos open new door for corporate hacking. Security researchers from Detectify Labs reported that companies in all industries may be at risk after finding that developers were leaving sensitive credentials inside open-sourced code following a scan on GitHub projects which revealed over 1,500 Slack access tokens were available online. The access tokens could allow attackers to access application program interfaces (APIs) and harvest user data, view Slack channel conversations, group information, private messages, and automate the use of Slack's search feature. <http://news.softpedia.com/news/slack-api-credentials-left-in-github-repos-open-new-doors-for-corporate-hacking-503527.shtml>

(International) Cisco finds backdoor installed on 12 million PCs. Cisco's Talos Security Intelligence and Research Group reported that a Tuto4PC's OneSoftPerDay application was discovered to install potentially unwanted programs (PUPs), harvest users' personal information, and was considered to be a backdoor for 12 million personal computers (PCs) after an analysis revealed that an increase in generic trojans were found when about 7,00 unique samples displayed names including "Wizz" in some of the domains. <http://www.securityweek.com/cisco-finds-backdoor-installed-12-million-pcs>

(International) Over 7M Minecraft mobile credentials exposed after Lifeboat data breach. Lifeboat Networks reported April 27 that its network was compromised in January, exposing its users' login names, passwords, and email addresses in the Minecraft Pocket Edition mobile game after a security researcher found over 7 million user credentials were available online. Lifeboat forced its customers to reset their passwords discretely and stated they started using stronger algorithms to guard user data. <http://www.scmagazine.com/over-7m-minecraft-mobile-credentials-exposed-after-lifeboat-data-breach/article/492634/>

(International) DDoS aggression and the evolution of IoT risks. Neustar released its findings after conducting a survey on over 1,000 information technology (IT) professionals across 6 continents which revealed that 76 percent of companies are investing in distributed denial-of-service (DDoS) protection as DDoS attacks are continuing to evolve from single large attacks to multi-vector attacks. Forty-

UNCLASSIFIED

UNCLASSIFIED

seven percent of attacked organizations were participating in information sharing on threats and counter measures to mitigate future assaults.

<https://www.helpnetsecurity.com/2016/04/27/ddos-aggression/>

(International) Facebook bug allowed attackers to take over accounts on other sites. Facebook patched a flaw in its account registration process after security researchers from Bitdefender discovered the flaw could allow attackers to take over users' profiles on Web sites where the Facebook Social Login feature was available by adding an attacker's email address as a secondary address, enabling the attacker to verify the profile and make modifications to the account information. <http://news.softpedia.com/news/facebook-bug-allowed-attackers-to-take-over-accounts-on-other-sites-503428.shtml>

(International) Compromised credentials still to blame for many data breaches. A Cloud Security Alliance survey found that a lack of scalable identity access management systems, a lack of ongoing automated rotation of cryptographic keys, passwords, and certificates, as well as failure to use multifactor authentication were the major causes of data breaches. The findings also indicated that 22 percent of companies who suffered a data breach, attributed the breach to compromised credentials. <https://www.helpnetsecurity.com/2016/04/25/compromised-credentials-data-breaches/>

PUBLIC HEALTH

(Florida) Twenty-five Miami-area defendants charged with submitting \$26 million in false claims to the Medicare Part D program. The U.S. Department of Justice and Florida officials announced charges April 28 against 25 Miami-area defendants in 3 separate cases for their alleged participation in various schemes to defraud Medicare of nearly \$26 million in false claims through the Medicare D program. The suspects reportedly submitted false claims for prescription drugs from at least eight Miami-Dade County area pharmacies that were not medically necessary and not provided to recruited Medicare beneficiaries. <https://www.justice.gov/opa/pr/twenty-five-miami-area-defendants-charged-submitting-26-million-false-claims-medicare-part-d>

UNCLASSIFIED

UNCLASSIFIED

(International) Windows XP, IE, and Flash Usage blamed for poor security of healthcare sector. Security researchers from Duo Security reported that many healthcare organizations were using outdated software or software prone to exploit kits (EK) after discovering that 33 percent of healthcare organizations were using Internet Explorer 11 rather than using updated versions of Google Chrome, and that 52 percent of healthcare organizations were using Flash Player software on all their computers, among other collected data.

<http://news.softpedia.com/news/windows-xp-ie-and-flash-usage-blamed-for-poor-security-of-healthcare-sector-503342.shtml>

TRANSPORTATION

(Washington, D.C.) Federal officials investigating Saturday's Metro track fire. Service between the Van Ness-UDC and Medical Center stations on Washington Metropolitan Area Transit Authority's Red Line was disrupted for several hours April 23 while Federal Transit Administration officials investigated a track fire near the Friendship Heights station in Washington, D.C. that sent smoke into a Metro tunnel, forcing passengers to evacuate. A preliminary investigation determined that the incident involved an insulator and was potentially the result of electrical arcing. https://www.washingtonpost.com/local/trafficandcommuting/metro-red-line-service-resumes-after-saturday-track-fire/2016/04/24/253c7a6e-0a2d-11e6-a6b6-2e6de3695b0e_story.html

WATER AND DAMS

(Illinois) Chicago to start testing water in some schools for toxic lead. The mayor of Chicago announced April 27 that Chicago Public Schools will begin initial tests for lead in water at 28 schools in order to help safeguard children. The results will be posted online and city officials will be given guidance as testing is expanded to include other schools. <http://www.chicagotribune.com/news/local/breaking/ct-cps-lead-water-emanuel-met-20160427-story.html>

UNCLASSIFIED

UNCLASSIFIED

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of Criminal Investigation (BCI):** 701-328-5500; **North Dakota Highway Patrol:** 701-328-2455; **US Attorney's Office Intel Analyst:** 701-297-7400; **Bismarck FBI:** 701-223-4875; **Fargo FBI:** 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165

UNCLASSIFIED