

# *the* Availability Digest

[www.availabilitydigest.com](http://www.availabilitydigest.com)  
[@availabilitydig](https://twitter.com/availabilitydig)

## **@availabilitydig – Our January Twitter Feed of Outages**

January 2018

A challenge every issue for the Availability Digest is to determine which of the many availability topics out there win coveted status as Digest articles. We always regret not focusing our attention on the topics we bypass. With our new Twitter presence, we don't have to feel guilty. This article highlights some of the @availabilitydig tweets that made headlines in recent days.



### **How Puerto Rico is Rebuilding Its Network Three Months After Maria**

It took less than 24 hours for Hurricane Maria to take Puerto Rico off the grid. The first Category 4 storm to hit the island since 1932, Maria knocked out power, shut down ports and left the entire territory completely in the dark. Once the storm passed, the government had to rely on physical messengers to assess the damage and to relay information across the island. Three months after Maria made landfall, rolled-back regulations, experimental technologies and portable satellite terminals have helped the government and private-sector restore communications across more than 85 percent of the island.

<https://t.co/Os5hnWgyA0>

### **Backing Up Big Data? Chances Are You're Doing It Wrong**

The increasing pervasiveness of social networking, multi-cloud applications and Internet of Things devices and services continues to drive exponential growth in big data solutions. As businesses become more data driven, larger and more current data sets become important to support the online business processes, analytics, intelligence and decisions. These big data solutions typically are built upon a new class of hyperscale, distributed, multi-cloud, datacentric applications. While these NoSQL, semi-structured, highly distributed data stores are perfect for handling vast amounts of big data, they no longer can be effectively supported by legacy data management and protection models. A different approach for backup and recovery is needed.

<https://t.co/cfWtxsggJm>

### **NASA and HPE Push the Envelope on HPC in Space**

Technology is rapidly transforming the way we think and understand the universe. In the realm of space science, technological advancements have enabled man to study Earth, explore new worlds, and even walk on the moon. Today, high performance computing (HPC) is accelerating space research and scientific discovery like never before. Organizations like NASA are using the most cutting-edge HPC solutions to analyze troves of complex data, conduct experiments, advance the Mission to Mars, and much more. NASA has teamed up with leading manufacturer Hewlett Packard Enterprise (HPE) to bring the most powerful earth-based systems into orbit in a mission called Spaceborne Computer.

<https://t.co/lgf4NVqhog>

### **Australia becomes World's First to Move Stock Exchange to A Blockchain**

The Australian Securities Exchange (ASX) has confirmed that it is to become the world's first global market to use blockchain technology to clear and settle trades. The distributed ledger will replace the outdated Clearing House Electronic Subregister System, also known as CHESS, that ASX currently uses. Even though ASX states that it continues to be a robust and reliable system, they are taking advantage of the opportunity to replace CHESS with a next-generation post-trade platform.

<https://t.co/zLStE8S4FP>

### **The 10 Biggest Cloud Outages Of 2017**

CRN's end-of-year list includes IBM, GitHub, Facebook, Microsoft Azure, and others.

<https://t.co/r8qdjUuDMC>

### **Everything you need to know about Serverless Computing**

The potentially game-changing technology of serverless computing isn't brand new; but like technologies before it such as containers, there's a few myths and misconceptions about it. To overcome this lack of insight into what to use serverless computing for, when not to use it, and how much it costs, CBR's James Nunns teamed up with Ian Massingham, Worldwide Lead, AWS Technical Evangelism at Amazon Web Services, to answer the big questions about the technology.

<https://t.co/eV6KbhnTSp>

### **IT infrastructure failing as if the past two decades never happened**

In Greek mythology, King Sisyphus was an arrogant ruler who believed he was smarter than Zeus. As punishment for his hubris, Sisyphus was tasked with pushing a boulder up a hill in the underworld, only to have it spin out of his control and roll back down. Based on recent data centre downtime events, we can only describe the process of keeping IT infrastructure running as Sisyphean. Data centre owners and operators repeatedly watch as the boulder slips from their grasp and back down the hill.

<https://t.co/ckN93apBtM>

### **Hardening Power Grids for Nuclear and EMP Attacks by North Korea**

Last month, federal agencies and utility executives held GridEx IV, a biennial event where officials responsible for hundreds of local utilities game out scenarios in which North America's power grid could fail. Potential calamities both physical and cyber are reviewed, with participant responses analyzed to better prepare for any future attack. This year, the event took on an added urgency given growing concern with a weapon straight out of the Cold War: an electromagnetic pulse, or EMP, emanating from a nuclear blast—specifically, one delivered by a North Korean missile or satellite detonated miles above the Earth. Though GridEx IV didn't pose this exact scenario, industry experts concede there's no clear plan to deal with it.

<https://t.co/bxFF5ZNVhk>

## Five Key Availability Predictions For 2018

Availability becomes increasingly important as businesses continue to increase their reliance on digital technologies and heavy dependence on the Internet. Applications and even consumer-facing services are now shifting to cloud and hybrid models as companies realize that in-house IT, once tasked with running an Exchange server and maintaining desktops, lack the tools and specialist expertise to keep these systems running.

<https://t.co/MbzUpDVYME>

## Elon Musk's massive Australian battery just chalked up another record

Elon Musk's battery in South Australia made international headlines in December for being the biggest of its type in the world. Then, just weeks after being activated, the very same battery claimed another world record for the time it took to spring into action following a power outage. The battery bounded into action just 140 milliseconds after a power plant in the neighboring state of Victoria suffered a failure that would ordinarily have led to a lengthy power cut. The battery fed its stored energy into the national power grid, preventing an inconvenient blackout from affecting numerous homes in nearby towns and cities.

<https://t.co/7UBtDDNsDS>

## Why your old network infrastructure is holding you back (more than you know)

*When communications infrastructure is not refreshed as often as end points, such as servers and mobile devices, limitations can quickly manifest.*

<https://t.co/IFtzSgCied>

## Civil Works Accident Brings Down Two Manchester Data Centers

More often than not, the specific event that triggers a data center outage is unpredictable. Companies spend tens of millions of dollars designing redundant infrastructure and automatic failover systems to compensate for the unpredictable. But that goal is unreachable by definition. A civil contractor accidentally drove a spike through a power main in Manchester, England, in early December. It cut off power supply to two of the three buildings on the data center campus operated by UKFast, the British service provider. The facilities' backup power system failed to do what it was designed to do, and the data centers went dark.

<https://t.co/UutokVZYVw>

## Apple's iPhones slowed to tackle ageing batteries

Many customers have long suspected that Apple slows down older iPhones to encourage people to upgrade. The company has now said it does slow down some models as they age but only because the phones' battery performance diminishes over time. The practice was confirmed after a customer shared performance tests on Reddit, suggesting his iPhone 6S had slowed down considerably as it had aged but had suddenly sped up again after the battery had been replaced.

<https://t.co/TvhnODNcO0>

## How MIT Students Fooled a Google Algorithm

Machine learning algorithms, which use large amounts of data to power everything from your email to language translation, are being heralded as the next big thing in technology. The only problem is that they're vulnerable.

<https://t.co/TN5CaGkmMM>

## Hewlett Packard Enterprise: A Company In Chaos

Despite reporting in-line results in Q4, HPE stock fell on news of CEO Meg Whitman's departure. 1) HPE fundamentals are still a complete mess, with declining revenues in its core server products. 2) The software business, once considered the lynchpin of HPE post-split, has been sold to MicroFocus for \$8.8 billion, eliminating a major growth driver for the company. 3) High memory prices, specifically for NAND flash, continued to eat into HPE's margins. 4) HPE lacks direction, and even new leadership won't be able to shake it up in the near term. Continue to avoid this stock, despite its new lows.

<https://t.co/y7MfuqGhji>

## Creating Chaos to Save the Datacenter

Downtime has been plaguing companies for decades, and the problems have only been exacerbated during the Internet era and with the rise of ecommerce and the cloud. Over the past several years, top hyperscalers and larger enterprises have started to break things in their infrastructures on purpose to smoke out weaknesses in the systems and to figure out how to harden them before failures catch them unprepared. Top-tier cloud service providers have become particularly vocal about the concept of chaos engineering, particularly given the multiple points of failure that are inherent throughout their massive and highly-distributed environments.

<https://t.co/mJIWUnU5xs>

## Atlanta airport had no plan for total power outage

While the airport had conducted drills for partial outages, making plans to shuffle operations between terminals, it made zero preparations for the entire facility to go dark. Among the airport's challenges: It had no electricity to power its public announcement system and only hundreds of employees to manage 35,000 stranded people. The airport's backup generators can power only one elevator per concourse. The generators in concourses D and E failed shortly after switching on.

<https://t.co/v8ABObUIHD>

## Atlanta airport's main and backup power lines flow through same tunnel damaged by fire

The fire that knocked out Atlanta airport's power for 11 hours Sunday, 17 December, erupted in a tunnel that housed both the main power lines and a backup supply, according to officials investigating the incident. The fire was traced to a failed switchgear, which is equipment that regulates the flow of power, in a tunnel that carries seven power lines from two sources to the airport. "This fire was located adjacent to the redundant circuit cables and switching mechanisms serving the airport; and those cables were damaged, resulting in the outage and loss of redundant service methods," Georgia Power explained in a statement.

<https://t.co/olmo1FSTlu>

## **How could one fire bring the world's busiest airport to a standstill? Even redundant systems can fail, engineers say**

How could one fire knock out the main power to Hartsfield-Jackson Atlanta International — the world's busiest airport — and at the same time disable the backup power, snarling air travel in the United States during one of the busiest travel times of the year? This is an airport, after all, that is supposedly among the most secure and locked-down facilities in a world where the threat of terrorism is an everyday reality. The short answer, according to engineering experts, is nothing is 100% certain when it comes to secure sources of electricity.

<https://t.co/myNS1fomne>

## **Resiliency in the age of cloud services**

Introducing cloud service redundancy starts with managing application workload: how do you direct work across multiple cloud service providers?

<https://t.co/51d00DlmcG>

## **Despite Security Vulnerability, Businesses Still Prefer Office 2007**

A new research study has found that over two thirds of companies are still opting to run Office 2007, which is software that Microsoft no longer supports. Spiceworks, an IT network that focuses on industry professionals, has found within its latest research that the majority of businesses are running Office XP, Office 2003, and Office 2007, while Microsoft pushes Office 365--a batch of subscriptions allowing access to several software including newer versions of Microsoft Office, etc.

<https://t.co/2W0RapWDWJ>

## **Is Your Website Ready for The Holiday Season?**

With the holidays just around the corner, have you prepared your website for a boost in traffic? This year, holiday online shopping is expected to surpass e-commerce sales in 2016 by 18-21%.

Whatever your product or service is, you need to prepare your website for heavy visitor spikes. Examples include: 1) **Use Full-Page Caching to Save Resources And Handle The Traffic**, 2) Take Advantage Of Object Caching If You Have Huge Databases, and 3) Use The Latest PHP 7.x To Make Your Site Faster And Lighter.

<https://t.co/fMqQ0aY511>

## **Three plead guilty to creating Mirai botnet used to crash web**

Three hackers have admitted to building the tools that attackers used to take down many of the Internet's most popular websites. One of the hackers admitted to writing the source code for Mirai -- malware that created a botnet that took over hundreds of thousands of computers and connected devices like security cameras and DVRs -- and using it to commit attacks and online fraud.

<https://t.co/CRLoyEUTrx>

## **Atlanta airport loses power, trapping travelers in planes and terminals**

A huge power outage brought the world's busiest airport to a standstill right before Christmas, ruining holiday travel for thousands. Atlanta Mayor Kasim Reed said a fire at the main substation powering the airport triggered the outage and caused the Federal Aviation Administration to put a ground stop in place, slowing or halting inbound air traffic.

<https://t.co/CTgXvd69Bg>

## **Norway becomes first country to end national radio broadcasts on FM**

Norway has completed its transition to digital radio, becoming the first country in the world to shut down national broadcasts of its FM network. The country's most northern regions and the Svalbard archipelago in the Arctic switched to digital audio broadcasting (DAB) as scheduled. The transition, which began on 11 January, allows for better sound quality and more channels and functions at an eighth of the cost of FM radio, according to authorities.

<https://t.co/g1ZWMn6ODF>

## **The Bots of Bitcoin**

The financial sector has taken steps to prevent computers accidentally bringing down the stock market; but the 2010 Flash Crash and others that followed underlie the dangers of relying on bots — or automated trading programs — to manage financial assets. Those bots are now active on cryptocurrency platforms. It's possible that if you've bought or sold Bitcoin or Ethereum, the buyer agreeing to take your order was not some cryptocurrency enthusiast in Silicon Valley but a piece of software on a server in Shanghai. It's not an entirely new development. In 2013, finance worker Joseph Lee launched trading platform BTC.sx after having made a reported \$150,000 in profit using scripted trading bots to buy and sell Bitcoin.

<https://t.co/P4Xvqj0W0s>

## **Real words or buzzwords? Five Nines**

What's wrong with 99.999% uptime? Recently, the author had several sales people mention high availability and state that Microsoft Azure guarantees them "five nines" of uptime, referring to their SaaS (Software as a Service) offering. There are several things wrong with this thinking.

<https://t.co/od17GNrCWI>

## **Who knew a tractor could cause so much trouble?**

Zimbabweans lost Internet access en masse in early December when a tractor reportedly cut through key fiber optic cables in South Africa, and another Internet provider experienced simultaneous issues with its primary Internet conduits. The outage began shortly before Noon local time and persisted for more than five hours, affecting not only citizens' day-to-day Internet usage but also businesses that rely upon web access. And while five Internet-free hours might sound unfathomable to those of us accustomed to having the web constantly at our fingertips, large-scale Internet outages—from inadvertent lapses caused by ship anchors to government-calculated blackouts designed to showcase political power—do happen and more frequently than you thought.

<https://t.co/dFdJ5YE9Pw>

## **Security system 'availability' jargon buster**

Does it really matter if software applications supporting your security systems are only available 99% of the time? Probably not if you've installed a video surveillance system primarily to deter shoplifters. But the loss of what equates to more than 90 minutes of unplanned downtime per week will be significant if you've invested in an integrated, mission-critical security solution. There is no shortage of solutions available to minimize disruption if a server fails or if you have to recover from a cyber-attack. Here is a jargon-busting overview of the best of them.

<https://t.co/u7OYjijqIH>

### **Brexit: failure to update customs system could be 'catastrophic'**

A failure to have a viable customs system in place to cope with Brexit when the UK quits the EU will be catastrophic for business and the reputation of the country, the government has been told.

The influential parliamentary public accounts select committee said it was deeply worried that Her Majesty's Revenue and Customs did not yet have the funding from the government to develop contingency plans for Brexit.

<https://t.co/UJAZ2U9Yu1>

### **Unsecured AWS server exposed classified military intel**

Sensitive military data found on an unsecured Amazon server belonging to the U.S. Army Intelligence and Security Command (INSCOM), a joint Intelligence effort with the National Security Agency, was accessible to the public. It included information on project Red Disk, an Army cloud-based intelligence platform, an auxiliary to the Distributed Common Ground System (Army DCGS-A), that failed.

<https://t.co/MuOjMVDyfl>

### **Software maintenance at the root of CBP's January outage**

A Department of Homeland Security inspector general's report examining a four-hour outage of the Custom and Border Protection's information technology system in January 2017 found that the agency had insufficient software testing and maintenance. The problem ultimately had to be corrected through legacy system servers, according to the report on the outage of CBP's Advanced Passenger Information System, which processes the ingress and egress of passengers to the U.S., utilizing information from the agency's TECS databases. The nationwide system crash caused significant flight delays, with the Office of the Inspector General reporting that 13,000 travelers were hindered by the outage in Miami International Airport alone.

<https://t.co/YwOBrO5to6>

### **Cloud-to-cloud backup: What it is and why you need it**

Applications that run in the cloud are protected but only so much. For full protection of data generated by cloud-based apps, you need cloud-to-cloud backup. Spending on public cloud services will reach US\$236bn by 2020, according to Forrester. It's a trend driven by increasing numbers of applications being delivered from the cloud. Cloud computing is sometimes so easy that users and IT teams assume it "just works," and they are happy to leave data protection and backup to the provider.

<https://t.co/N3m6Fd7dqU>

### **HP laptops found to have hidden keylogger**

Hidden software that can record every letter typed on a computer keyboard has been discovered pre-installed on hundreds of HP laptop models. Security researcher Michael Myng found the keylogging code in software drivers preinstalled on HP laptops to make the keyboard work. HP said more than 460 models of laptop were affected by the "potential security vulnerability." It has issued a software patch for its customers to remove the keylogger. The issue affects laptops in the EliteBook, ProBook, Pavilion and Envy ranges, among others. HP has issued a full list of affected devices, dating back to 2012.

<https://t.co/Bx0VEHCvsr>

### **Here's What We Know About Google's Chromebook Internet Outage**

Around 2:30 p.m. on Tuesday, December 5<sup>th</sup>, Adam Henderson began receiving from across his district's 17 schools a flood of reports saying that Chromebook devices were no longer working. Henderson, who is the Director of Technology Systems at Nassau County Schools in Florida, was among the many educators who experienced the issue, which caused Chromebook devices to logout of existing Internet accounts and fail to reconnect. In Nassau County, 5,000 devices experienced the outage; but it's expected that tens of thousands and perhaps millions of devices around the country could have experienced the same glitch.

<https://t.co/16Vvf7XTMs>

### **Computer outage at hospitals, health centres caused by hardware, software failures**

In early December, a computer outage that forced staff at hospitals and health-care centres across the New Brunswick (Canadian province) to cancel services and turn patients away was blamed on hardware and software failures in the data storage system. About 140 computer systems at Horizon and Vitalité health authorities were unavailable during the outage, including provincial systems such as the drug information database and regional systems such as patient scheduling and oncology treatment systems.

<https://t.co/hnzhpkeOGN>

### **Bitcoin mining company says it was hacked, possible theft worth millions**

A bitcoin mining company in Slovenia said in December that it had been hacked for the possible theft of tens of millions of dollars. As the price of the virtual currency soared past \$17,000, NiceHash, a company that mines bitcoins on behalf of customers, said it is investigating a security breach that may have resulted in the theft of about \$70 million worth of bitcoin.

<https://t.co/ekZ6HO3MsR>

### **North Carolina County Refuses to Pay \$23,000 Ransom to Hackers**

In a world rocked by hackers, trolls and online evildoers of all stripes, the good people of the Internet have long looked for a hero who would refuse to back down. Finally, someone has said enough is enough. And that someone is the government of Mecklenburg County, North Carolina (U.S. State). Mecklenburg is the most populous county in North Carolina, and the attack compromised many of its systems. But after the ransomware attack, it said it was "open for business, albeit somewhat slower with limited access to systems."

<https://t.co/tTkRw6Q2uP>

### **New global Internet reliability concerns emerge**

Undersea, Internet-carrying cables are not protected well enough; and there isn't an alternative in place should they fail. That's according to a new report from U.K.-based Policy Exchange, which outlines potential catastrophic effects that a simple cut in the hosepipe-sized underwater infrastructure could create.

<https://t.co/SNW1aVqTjW>

### **Stratus unveils edge computing strategy**

With more than 90 percent of industrial companies wanting a simplified edge infrastructure that can be remotely managed, Stratus Technologies, a global leader in continuous availability solutions for mission-critical applications, recently unveiled its edge computing product strategy. This strategy includes the latest version of Stratus' flagship product, ftServer, along with a preview of a converged edge system, which offers enhanced remote management services in a rugged and easy-to-deploy form factor.

<https://t.co/BhiR0MRv4d>

### **Here's How the Army Plans to Survive Space Attacks**

U.S. military equipment relies heavily on satellites for GPS, but the Army is working on backup plans in case a space attack disables GPS service. The Pentagon is not only working to reintroduce paper maps, but it is also preparing for an impact that moves far beyond interrupted navigation. For example, disrupted GPS and satellite communications will threaten the operation of drones and munitions such as the Joint Direct Attack Munition (JDAM), which is in part guided by satellite.

<https://t.co/gNXjMIQIKR>

### **NASA fixes Voyager 1 deep space probe by firing thrusters not used in 37 years**

Voyager 1 was launched in September 1977 and is the only human-made object in interstellar space - the environment between the stars. But after four decades of exploration that have taken in fly-bys of Jupiter and Saturn, engineers found that the primary thrusters orienting the space probe had severely degraded. In an attempt to keep Voyager 1 operable, NASA tested four thrusters on the back side of the spacecraft, thrusters that have not been used since 1980. After waiting more than 19-and-a-half hours for test results to travel through space, engineers found the dormant thrusters had worked "perfectly." NASA now plans to use the trajectory correction maneuver thrusters permanently - giving Voyager 1 an extra two to three years of life.

<https://t.co/OPLGKLRS0D>

### **Tesla mega-battery in Australia activated**

The world's largest lithium ion battery has begun dispensing power into an electricity grid in South Australia, which has been crippled by electricity problems in recent times. Tesla boss Elon Musk famously vowed to build the battery within 100 days - a promise that was fulfilled. Located near Jamestown, about 200km (125 miles) north of Adelaide, the battery is connected to a wind farm run by French energy company Neoen.

<https://t.co/NFveXw3e2L>