

the Availability Digest

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

@availabilitydig – Our October Twitter Feed of Outages

October 2014

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.



A Troubled Project To Replace Oracle With SAP Software Could Cost A New York Gas Utility Nearly \$1 Billion.

National Grid, a New York gas utility service, may be charged nearly \$1 billion for a flawed project that failed to upgrade its internal payroll systems in time.

<http://t.co/JO118476Rj>

Stratus provides always-on solutions for even the world's busiest airport! Check out how we did it.

For the past five years, Hartsfield-Jackson has depended on Public Safety Systems Incorporated (PSSI) and Stratus Technologies to keep its computer-aided dispatch CAD system running smoothly with maximum availability.

<http://t.co/gzlxHY40nA>

The new "HP NonStop for Dummies" presents a "concise, short overview of the HP NonStop platform."

Keeping up with technology trends is hard in itself - dealing with a platform that has a legacy of nearly 40 years might be even more of a challenge. Of course; there is a wide range of public information available on HP NonStop; but to the best of our knowledge, there was no platform primer available prior to this book.

<http://t.co/tMDbvkykSQ>

Five Ways Cyberterrorists Could Target The U.S.

Will the next terrorist attack occur in cyberspace? Cyberwarfare is now largely seen as an integral part of modern warfare by most developed nations, and countries like the US, Russia, and China spend hundreds of millions of dollars per year developing these capabilities.

<http://t.co/8iu1jnuOjk>

How one user (successfully) managed the Amazon cloud reboot.

PropertyRoom.com is an online auction site of seized goods that is run entirely on Amazon Web Services' cloud. Late last week, AWS announced that it would be rebooting up to 10% of the company's virtual machines, known as its Elastic Compute Cloud (EC2) instances. For a company like PropertyRoom.com, which processes tens of millions of dollars worth of online auctions all through Amazon's cloud, that could have been a big problem.

<http://t.co/8rXkCrFZTL>

FAA: Upgrading air-traffic control will reduce disruptions.

A fire that knocked out air-traffic control across a five-state region around Chicago last Friday revealed the fragility of current navigation equipment. The Federal Aviation Administration is upgrading the system, but the process will cost billions of dollars and require decades to complete.

<http://t.co/UuZVatJQG6>

Physical Layer Management for Hosting Companies

Physical layer management (PLM) systems provide the real-time view of the physical network needed to improve hosting service provider uptime and customer service.

<http://t.co/mHUqHPTtT9>

Sweden: Bitcoin is wild west, but it could be a central bank's backup plan.

Bitcoin usually gets slapped with a 'high risk' label, but a Swedish economist reckons it could actually have a stabilizing effect under some circumstances.

<http://t.co/Jb2a85KHd3>

Belkin apologizes for mass router disconnections.

Belkin has apologized to its customers following a server outage that knocked selected models of routers off the internet. The issue was traced to a particular host, heartbeat.belkin.com, which the routers regularly ping to verify connectivity. With a network failure taking this host offline, many routers decided they were without a working internet connection and promptly stopped attempting to resolve hostnames via DNS.

<http://t.co/rDgLc8q6vo>

Digest Mg Ed Bill Highleyman speaks on "DDoS Attacks Can Take Down Your Online Services." Wed, 8 Oct., Continuity Insights New York 2014.



DDoS Attacks Can Take Down Your Online Services Part 2: DDoS Attack Strategies.

In Part 2, we describe some of the various attack strategies that may be used in a DDoS attack. Of note is that the attacker often monitors the success of its attack. If it finds that its attack is not having the effect anticipated, the attacker can change strategies until it finds a successful way to take down the victim system.

<http://t.co/zOXXMoXbRC>

Serious about cloud? Follow Netflix's lead and get into chaos engineering.

Netflix is demonstrating that companies thinking of moving to cloud infrastructure need to build their systems to fail.

<http://t.co/UbgIfH77K1>

What can we learn from the 2014 Verizon Data Breach Investigations Report?

This is the tenth year that Verizon has issued its Verizon Data Breach Investigations Report (DBIR). The DBIR analyzes reported security incidences, data breaches (those in which data was exposed), and confirmed data disclosures (those in which information was actually stolen).

<http://t.co/9pQKeXQwms>

HealthCare.gov delays Web host switch.

The U.S. government has shelved plans to move the HealthCare.gov insurance website to a new host for the coming enrollment period, delaying a move that was supposed to fix reliability problems.

<http://bit.ly/1nzqDuo>

Auckland's 5th major outage since 1998

The biggest Auckland, NZ, outage was the six-week Mercury power outage in 1998 and involved the failure of four power cables due to overheating. The most recent outage took out 85,000 businesses and households. It was caused by a fire in a cable trench on at a sub-station, a site shared by the local network owner Vector and the national grid operator, Transpower.

<http://t.co/EL1XRh4KCH>

Contact Lost With Planes One by One as FAA Fire Spread.

The first radio links with pilots were lost just as the pre-dawn crush of flights into Chicago began. Air-traffic controllers in an Federal Aviation Administration building switched to backup channels. Then those failed. Controllers tried emergency connections, which also went dead. Within minutes, radar feeds, flight plans and other data that controllers rely on to direct more than 6,000 aircraft a day had vanished because of a fire deliberately set in a communications room one floor below.

<http://t.co/VWIVpLI5Tc>

How Netflix survived the Amazon EC2 reboot.

Sometimes the best path to success is to learn how to avoid failure. Netflix was able to keep serving its customers while its cloud hosting provider, Amazon Web Services (AWS), rebooted servers, because Netflix had prepared for that happening.

<http://t.co/NmW7f0xr45>

When the backup fails. "Delays at O'Hare, Midway after Indianapolis FAA outage."

Airline delays at Chicago airports surged on 6 October due to a telephone outage at an Indianapolis air-traffic control facility that is handling flights normally managed by the idled Aurora radar center, which has been offline since a fire was intentionally set on 26 September. The telephones in Indianapolis typically are used as backup for communicating with controllers elsewhere.

<http://t.co/mZeowXBKIA>

From the Availability Digest: Where does stolen information go? To the Darknet!

Over a three-week period at the end of 2013, Point-of-Sale (POS) terminals at U.S. Target stores were infected with malicious software that stole the personal information of over 110 million credit-card holders. Yet another American retailer, Home Depot, recently announced its POS terminals were hacked. Question: What happens to all that stolen information? Answer: It is offered for sale on the Darknet.

<http://t.co/QvzU3iEJy4>

The Internet Is Broken, and Shellshock Is Just the Start of Our Woes.

Shellshock is one of the oldest known, unpatched bugs in the history of computing. It was typed into the "ancient" code Bash, a program that was built for Unix and is now found in tens of thousands of machines. Last week, more than twenty years after Bash's development, security researchers finally noticed the Bash flaw. They call it Shellshock, and they warn it could allow hackers to wreak havoc on the modern Internet.

<http://t.co/TC1YN1qbko>