the Availability Digest

www.availabilitydigest.com
@availabilitydig

@availabilitydig – Our June Twitter Feed of Outages

June 2017

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.

Recent Chase Outage Cripples Mobile Payments for Hours

Recently, JPMorgan Chase customers experienced an outage that included online bill pay and the Chase QuickPay mobile payments service, which handles the increasingly popular peer-to-peer (P2P) payments service. The services cut out around four in the afternoon but were brought back around 8:30. Four and a half hours without bill pay and mobile payments isn’t exactly good news; but for most, it was a safe bet that disruption was minimal. For Chase, however, which lost out on a bunch of payments to process and cash accordingly as well as a loss of face in the market the losses were much greater.

https://t.co/jQep2bJWJc

Preparing for the Cyberattack That Will Knock Out U.S. Power Grids

Cyberattacks are unavoidable, but we’re not going to stop using computerized systems. Instead, we should be preparing for the inevitable, including a major cyberattack on power grids and other essential systems. This requires the ability to anticipate not only an unprecedented event but also the ripple effects that it could cause.

https://t.co/G8yl4ErWph

LPL Financial Hit by System-Wide Technology Outage

May 12th’s global cyber-attack by unknown hackers across numerous businesses around the world wasn't the only negative technology-related development. Less widely publicized was a system-wide technology outage at one of the country's independent broker-dealers, LPL Financial. At some point on Friday, LPL's 15,000 advisors were no longer able to access its Charlotte, N.C.-based data center, causing much of the firm's technology platform to become unusable. As the outage unfolded, the company's phone systems were unable to keep up with demand, leaving many LPL-affiliated advisors in the dark.

https://t.co/FrbXqKGyxZ

EE down: 4G outage leaves thousands of customers without service across UK

BT-owned mobile operator EE recently experienced an outage with its 4G mobile data coverage. The outage affected thousands of customers across the UK. The 4G service blackout, identified by EE as a “data issue,” affected customers in London, Birmingham, Streatham, Manchester, Leicester, Leeds, Sheffield, Hull, Glasgow, and Nottingham.

https://t.co/3X3AobStFc

Starbucks computers crash in widespread outage

Large parts of the United States and Canada were impacted by a coffee shortage as a result of a crash to Starbucks's computer systems in mid-May. The caffeine crisis began on a Tuesday morning and as of mid-afternoon remained unresolved. The company acknowledged the problem, saying it was the result of troubles with a software update, not hacking. A Starbucks spokesperson said the problem came about as a result of a "technology update" to store registers and that a limited number of the country's 14,000 North American locations were affected.

https://t.co/6FlBCmYo7m

Orlando airport shuttle debacle was crash of history, glitches and surprise

Recent malfunctions with Orlando International Airport’s new shuttle provoked astonishment that a broken train could trigger such a debacle for which there was no immediate rescue plan. The episode was one of the most severe growth pains ever suffered at the airport, which is the nation’s 14th busiest and is amid a daunting, $3.1 billion expansion in gates, trains and garage space.

https://t.co/kkplGeKMn1

Yahoo’s Bob Lord said massive data breach felt like Vertigo

Being the chief information security officer at the company that’s suffered the biggest (known) data breaches in history isn’t the kind of fame most CISOs would be looking for. But it’s Yahoo’s Bob Lord’s bag. Last fall, Yahoo revealed that a state-sponsored hack had affected at least 500 million accounts, with (as it turned out) the information stolen at least as early as January 2014 and utilized until at least December 2016. The news of that huge hack was topped a few months later when Yahoo also revealed it had suffered an even more massive hack in August 2013 of more than one billion user accounts.

https://t.co/6gyRsrUova

An Interesting Tidbit: Dinosaur asteroid hit 'worst possible place'

Scientists who drilled into the impact crater associated with the demise of the dinosaurs summarise their findings so far in a BBC Two documentary. The researchers recovered rocks from under the Gulf of Mexico that were hit by an asteroid 66 million years ago. The nature of this material records the details of the event. It is becoming clear that the 15km-wide asteroid could not have hit a worse place on Earth. The shallow sea covering the target site meant colossal volumes of sulphur (from the mineral gypsum) were injected into the atmosphere, extending the "global winter" period that followed the immediate firestorm. Had the asteroid struck a different location, the outcome might have been very different.

https://t.co/gxLZ4ATDsM

Is Microsoft to blame for the largest ransomware attacks in internet history?

May 2017 saw the largest global ransomware attack in internet history, and the world did not handle it well. We're only beginning to calculate the damage inflicted by the WannaCry program; but at the same time, we're also calculating blame. There's a long list of parties responsible, including the criminals, the NSA, and the victims themselves — but the most controversial has been Microsoft itself. The attack exploited a Windows networking protocol to spread within networks; and while Microsoft released a patch nearly two months ago, it's become painfully clear that patch didn't reach all users. Microsoft was following the best practices for security and still left hundreds of thousands of computers vulnerable, with dire consequences. Was it good enough?

https://t.co/NY5yGXvohM

Digest Oldie but Goodie: "The Alaska Permanent Fund and the $38 Billion Keystroke"

Do you ever have that sinking feeling just before you depress the delete key? Am I deleting the correct file? Can I recover it if I'm wrong? An employee of the Alaska Department of Revenue perhaps should have thought twice before acting. While maintaining a system that distributed oil revenues to Alaskans, he made one fateful keystroke that totally wiped out an account worth $38 billion – and its backup!

http://bit.ly/2r99kav

U.K. Health Service Ignored Warnings for Months

Britain's National Health Service ignored numerous warnings over the last year that many of its computer systems were outdated and unprotected from the type of devastating cyberattack it suffered in May. Many of the N.H.S. computers still run Windows XP, an out-of-date software that no longer gets security updates from its maker, Microsoft. A government contract with Microsoft to update the software for the N.H.S. expired two years ago.

https://t.co/Wmi03lMrLO

Microsoft issues 'highly unusual' Windows XP patch to prevent massive ransomware attack

UK hospitals, Telefonica, FedEx, and other businesses were hit by a a massive ransomware attack in May. Around 75,000 computers in 99 countries were affected. The malware was able to spread thanks to flaws in old versions of Windows. While Microsoft quickly issued fixes for the latest versions of Windows last month, this left Windows XP unprotected. Many of the machines attacked were breached simply because the latest Windows updates had not been applied quickly enough, but there were still organizations that continue to run Windows XP despite the risks. Microsoft is now taking what it describes as a "highly unusual" step to provide public patches for Windows operating systems that are in custom support only. This includes specific fixes for Windows XP, Windows 8, and Windows Server 2003.

https://t.co/dJpfGOwsz8

Cyber attack: RBI asks banks to shut down ATMs till software is updated

In May, the RBI (Reserver Bank of India) directed banks to operate their ATMs only after the installed computer systems received a special Windows update to protect them from a malware impacting systems across the world. This directive came in the wake of global system outages due to WannaCry ransomware.

https://t.co/AfxNh5rG7a

Solar Mini-Grids Could Shield The U.S. From Terrorist Strikes

The diversification of energy sources that feed the American electric grid should be a national security priority to ensure a robust national grid system that can withstand natural disasters and terrorist attacks on U.S. infrastructure. But according to a new paper by the Michigan Technological University (MTU), that's not enough. The experts said that building resilience to cascading blackouts, attacks from hostile foreign entities and other grid-threatening events requires the wide-scale development of solar resources while creating independently functioning micro-grids that will retain their ability to produce power in case of a mass outage. And the American military concurs.

https://t.co/f7NopyNzWJ

NHS hack part of huge global attack that has crippled 36,000 machines

A global cyber-attack using hacking tools widely believed to have been developed by the US National Security Agency and leaked online by a group called the Shadow Brokers caused chaos around the world in May. British hospitals, the Russian government, German railways and big companies like FedEx were among those affected when they were crippled by the 'ransomware' that rapidly spread across the globe and infected 75,000 computers in 99 countries.

https://t.co/ASjM4eBkcb

There's a Massive Ransomware Attack Spreading Globally Right Now

In May, a ransomware attack quickly spread across the globe and rendered vital systems inaccessible. "In less than 3 hours (even can say less than 2 hours if we count it from the explosion), victims already were found in 11 countries." Approximately 6 hours later, Kaspersky Lab reported more than 45,000 attacks in 74 countries.

https://t.co/M82jPEJS3W

San Francisco, Los Angeles Outages Highlight Growing Risks, Rising Costs of Aging Power Infrastructure

San Franciscans and Los Angelenos alike suffered through major power failures in April. Given California's national and world leading role in fostering deployment of a new generation of distributed solar, renewable energy, energy storage and smart grid technologies, some may be tempted to use the Los Angeles (LA) and San Francisco (SF) grid failures to highlight the high risk and potential costs of aggressively pursuing such a proactive new power and energy market reform agenda.

They'd be mistaken in doing so. Rather, the SF and LA power grid outages were the result of "run of the mill" equipment failures that have been responsible for bringing down electricity grids since the dawn of the industry.

https://t.co/NFQXqNPibu

Chase outage knocks out payments service for customers nationwide

JPMorgan Chase customers nationwide on Thursday 11 May were prevented from making online and mobile payments due to unspecified technology issues. Services including bill pay and Chase QuickPay — the company's peer-to-peer payment service — went down around 4 p.m. and were restored around 8:30 p.m.

https://t.co/F6OCH9LvKF

At least 16 hospitals now completely offline after huge hack

A huge cyber-attack infected NHS trusts across the U.K. in May and led to all digital systems being pulled down. The ransomware threatened hospitals that they would lose access to patient records and other files if they didn't pay money to the hackers. The attack used the Wanna Decryptor variant of malware, which holds affected computers hostage while the attackers demand a ransom.

https://t.co/9FV46rdpFv

Digest Oldie but Goodie: "The Cost of RPO and RTO"

The purpose of availability analysis is to determine how to limit downtime and data loss. Both cost a corporation money and reputation. But improving them also costs money. Improvement generally means adding redundancy to the corporate systems. How does one balance the cost of availability improvement against the savings of reduced downtime and lost data?

https://t.co/lNMnnk3po1

IBM Bolsters Disaster Recovery with GDR For IBM i

In June, IBM plans to start selling a new disaster recovery product to IBM i shops. Called Geographically Dispersed Resiliency, or GDR, the new offering is designed to give companies an easy and affordable way to recover production IBM i LPARs on remote machines.

https://t.co/qNft6sLDK9

New Mirai-like threat, dubbed Persirai, targeting online IP cameras, warns Trend Micro

A new Internet of Things (IoT) threat has been uncovered by security firm Trend Micro. Dubbed Persirai, it has reportedly been infecting particular Chinese-made wireless cameras for around a month. The Mirai-like threat, which is said to have infected 120,000 IP cameras so far, exploits flaws in the cameras. What's more, owners of affected cameras are unlikely to know that they have been affected.

https://t.co/QUlfeA5any

Karachi plunges into darkness as Bin Qasim power plant trips

A large part of localities plunged into darkness on a Tuesday night in May as a major fault occurred at the Bin Qasim electric power plant. Power distribution in five districts of the city was adversely affected as result of the tripping, causing power outage for hours. The power utility failed to restore the electricity through 12 grid stations to the affected areas till Wednesday morning. It was the third major breakdown recently in Karachi.

https://t.co/FIaHo1BcuP

Is Estonia a Preview of Our Tech Future?

"On a Spring afternoon, I'm gazing out the window of an office building on the outskirts of Estonia's capital, Tallinn, watching people stroll below, when a cream-colored plastic container mounted on black wheels rounds the corner and begins maneuvering its way among the pedestrians. The device looks like a kid's toy. But in reality, it's a high-tech delivery robot called Starship and potentially the next mega-profitable invention to spring from this snowy, miniature country on the northern edge of Europe—one of the more unexpected launching pads on the planet." Fun fact: Skype was invented in Estonia.

https://t.co/odeDNpLf3O

Why veteran of a legacy vendor joined core banking startup crowd

The number of cloud-based core banking startups is on the rise. The latest is Finxact, which formally launched in May. For founder and CEO Frank Sanchez, this is a return to his roots. In the early 1980s, Frank Sanchez and his brother Mike started Sanchez Computer Associates and created a core banking system called Profile. They sold the system to several Eastern European banks, then sold the company to FIS in 2004. Sanchez then ran the Enterprise Banking Division at FIS for eight years.

https://t.co/EFHCPt7LBn

Twitter down, users unable to post as micro-blogging site faces temporary outage for second day

Micro-blogging website Twitter on 10 May faced a temporary outage for the second consecutive day. Users were unable to make any posts while the social networking website was down. On Tuesday, 9 May, Facebook and Twitter both faced temporary outages.

https://t.co/N87LTzWyY1

Preparing the Nation for Intense Space Weather

The entire Canadian province of Québec, which covers twice as much area as the U.S. State of Texas, was plunged into darkness on the morning of March 13, 1989. An intense geomagnetic storm seized Québec's power-grid system, tripping relays, damaging high-voltage transformers, and causing a blackout. This geomagnetic storm's impact on Québec pales in comparison to what could happen in the future. A report by the National Academy of Sciences suggests that a rare but powerful magnetic superstorm could cause continent-wide loss of electricity and substantial damage to power-grid infrastructure that could persist for months and cost the nation in excess of $1 trillion.

https://t.co/VEEN7Mi0Ic

GE patches flaws allowing attackers to 'disconnect power grid at will'

Researchers have discovered a significant software flaw in the energy grid equipment sold by General Electric (GE) that could allow even lone attackers with limited resources to "disconnect sectors of the power grid at will." In May, GE announced that it had issued fixes for five of the six flaws, with the last on its way.

https://t.co/iLyVDekL19

Installing solar to combat national security risks in the power grid

Solar technology could help make the power grid more resilient to attacks and natural disasters. Many military bases are located in regions with a history of power outages. Microgrids could serve as back-ups to prevent service disruption during natural disasters and attacks.
https://t.co/SThBHjvUSO

Cartu Bank Ensures Continuous Availability of Payment Services for Georgian Businesses

Cartu Bank understands the need for continuous availability with more than 60% of all e-commerce transactions in the Eastern European country of Georgia going through its payment switch. Read this HPE case study to learn how HPE NonStop servers with HPE Shadowbase software run mission-critical BASE24 payment engines to keep the Georgian economy running 24×7.

https://t.co/Qg2E7iGxXq

Spy agency back-up generators failed during power outage

Back-up electricity failed at Australia's electronic spy agency that prevents national cyber-attacks when a cable fault cut off energy supply in January. Defence officials told a parliamentary inquiry hearing that the Australian Signals Directorate lost electricity from ActewAGL, and back-up generators failed to power one of its two buildings for two hours during the outage. The ASD is relying on diesel generators needing parts no longer manufactured to prevent a power shut-down.

https://t.co/0vqinpLVyB

If it's not poltergeists or the Russians, it could be your power utility

Here's a mystery for your wall of weird. All of a sudden, six battery backups died at the same time (with no visible power problems). Read on to learn how we solved the mystery and how six brave little UPSs gave their lives in service to geekdom.

https://t.co/lScydT4JaN

Southwest Braces for Upgrade of 30-Year-Old Reservations System

Southwest Airlines Co. plans to shift its domestic reservation system to a new platform in early May, attempting to avoid the havoc that plagued similar transitions at other carriers. Southwest is spending $500 million, its biggest technology update ever, as it moves from a 30-year-old system. The Dallas-based company began using the new tools in December to book customers who were traveling May 9 and later to phase in the transition. The three-year process has included extensive employee training and months of testing. (Note: transition was successful)

https://t.co/QXQO1pKaSK

HPE tells Nutanix 'we're not partners' in software scuffle

HPE has made clear to customers that it is not partners with Nutanix after the latter opened up its Enterprise Cloud Platform software to allow users to install it on HPE ProLiant and Cisco UCS B-series servers.

https://t.co/K9n4xgUGpk

Key to Improving Subway Service in New York? Modern Signals

At a subway station deep under Manhattan, a dingy room is filled with rows of antique equipment built before World War II. The weathered glass boxes and cloth-covered cables are not part of a museum exhibit. Instead, they are crucial pieces of the signal system that directs traffic in one of the busiest subways in the world. Much of the signal equipment at that station, at West Fourth Street, is decades beyond its life span; and it is one of the main culprits plaguing the overburdened subway.

https://t.co/g8zkM6ulWe

Banks should let ancient programming language COBOL die

“This extremely critical part of the economic infrastructure of the planet is run on a very old piece of technology — which in itself is fine — if it weren’t for the fact that the people servicing that technology are a dying race.”

https://t.co/hIqz4BrSeE

Antiquated crew-tracking system at the root of another major Delta tech debacle

Delta Airlines’ crew-tracking system fell apart when a series of thunderstorms hit the Atlanta area in early April, causing flight to be delayed or cancelled. The breakdown prevented the airline crews from receiving assignments from Delta’s operation center, making the situation much worse and eventually resulting in 4,000 cancellations. In many cases, crews didn't show up for flights, because they were unaware of their assignment.

https://t.co/NIoof4XBOk

The plan to make America’s nukes great again could go horribly wrong

It was nearly 2 o’clock in the morning on Oct. 23, 2010, when an Air Force lieutenant called from his base in Wyoming to report the nightmare scenario unfolding before him. Fifty intercontinental ballistic missiles — each tipped with a nuclear warhead 20 times more powerful than the bomb the U.S. dropped on Hiroshima — had suddenly lost contact with the computers at the base’s launch center.

https://t.co/t8tatybn3G

Four nines and failure rates: Will the cloud ever cut it for transactional banking?

Banks looking to take their cloud plans to the next level are likely to have returned to the drawing board following the latest Amazon Web Services outage, which disrupted the online activities of major organizations from Apple to the US Securities and Exchange Commission. One estimate suggests US financial services companies alone lost $160 million – in just four hours. It’s been a timely reminder that any downtime is too much in an always-on digital economy, certainly for financial services. The sobering point is that AWS was still delivering within the terms of its service-level agreement (SLA). This promises 99.99% service and data availability (otherwise known as “four nines” availability). This may be good enough for a lot of things, but it won’t do for banking.

https://t.co/RQPX6AJ4M4

WhatsApp Back Online After Global Outage

WhatsApp went down, and the world went a little nuts. Literally, the world. Widespread outages were first reported around 4 p.m. Wednesday, May 3rd. The problem was mostly resolved by 7 p.m. the same night. But during that time, no one on the planet could use WhatsApp. And that’s a lot of people. WhatsApp is considered the world’s second largest social media platform, though it’s largely used as a messenger app. At last count, it has 1.2 billion active users monthly. It’s only beaten by Facebook, which owns WhatsApp.

https://t.co/BWDWQNk1ng

Blockchain: The smart person's guide

This comprehensive guide covers everything you need to know about the blockchain, the innovative technology that powers Bitcoin, Litecoin, and other cryptocurrencies.

https://t.co/v54sANWAIe

From Good to Great: The Path to 99.5 Percent to + 99.9 Percent System and Application Uptime

We can thank SaaS providers for raising the bar with regard to system and application availability. Today, while 99.5% system and application uptime is considered “standard” by most cloud providers, this equates to 3.42 hours of downtime per month – a significant speed bump in today’s always–on business environment. Increasingly, this “min” bar is being raised to 99.9% - a figure which equates to 38 minutes (or less) of downtime per month. How will IT organizations meet this uptime imperative without significantly increasing costs?

https://t.co/mOfPL4MZD2

The Evolution of High Availability

The traditional view of designing for and achieving high availability systems has been concentrated on hardware and software. Recently, people have recognized the importance of ‘fat finger’ trouble causing outages. If we can minimize the hardware and software issues and reduce finger trouble by rigorous operations procedures, then the problem is solved. Or is it? There are other factors which are either not recognized or understood.

https://t.co/P9lvY70ArX

The 7 worst automation failures

There are IT jobs that you just know are built for failure. They are so big and cumbersome and in some cases are plowing through new ground that unforeseen outcomes are likely. Then there are other situations where an IT pro might just say “whoops” when that unforeseen result should have been, well, foreseen.

https://t.co/6guRUFT9ut

Feds: Human Error, Labeling Led to Chemical Cloud in Kansas

Human error and labeling and design problems led to the release of a large chemical cloud over a city in the U.S. state of Kansas in 2016. The incident sent more than 140 people to the hospital and caused others to stay indoors or evacuate for several hours.

https://t.co/tx0EN3zmMD

The Human Factor: The unspoken threat in cybersecurity

Ever since there have been humans, there have been human errors – and some of them have been whoppers (like the Japanese trader's “fat finger” trading error that cost his company $600 billion). Doing tasks that they really don't understand or mistakenly pushing a button or pulling a lever, people are the root cause of 90% of air traffic control errors, over 50% of factory equipment failures after maintenance, 37% of downtime at pharmaceutical firms, and in one of the biggest flubs of all time, human error nearly destroyed Kansas. Such errors can destroy a company, too – by allowing hackers access to sensitive data.

https://t.co/st0H7ukXaZ

SAN outages put dent in ATO's cybersecurity

The high-profile failure of an ATO (Australian Taxation Office) storage area network (SAN) left the tax office struggling to be compliant with its IT security obligations. A submission by the ATO to the joint committee of public accounts and trust shows while the agency had been tracking well to meet the ASD's top four mitigation strategies this year, the well-documented SAN failures put a dent in its overall IT security profile.

https://t.co/Igcqi1fXQa

Block Island to start getting wind power

In early May, Block Island (in U.S. State of New York) formally throw the switch on a first-time connection to the New England energy grid through a new cable to the mainland and begin receiving power from the country’s first five offshore wind turbines. It will end nearly a century of dependency on loud, smoky diesel-fired power generators that burn about 1 million gallons a year.

https://t.co/SW6eNtSiab