the Availability Digest

www.availabilitydigest.com
@availabilitydig

@availabilitydig – Our December Twitter Feed of Outages

December 2016

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.

Why Southern China Broke Up Its Power Grid

Throughout the 20th century, utilities merged transmission systems with neighboring grids, creating ever-larger AC electricity grids. Some, such as Europe's and North America's, now approach continental scale. But a recent move in China to break up an AC grid suggests that growing use of DC transmission technology may turn back the clock.

https://t.co/8yXwyawVs8

Deutsche Telekom Internet Outage Blamed on Mirai Botnet

Hundreds of thousands of Deutsche Telekom customers in Germany faced Internet outages in late November following a widespread Internet of Things attack from the so-called Mirai botnet. Deutsche Telekom on Monday said 900,000 customers suffered outages as a result of a botched router attack. "The attack attempted to infect routers with a malware but failed, which caused crashes or restrictions for four to five percent of all routers," the company said, adding that its network was not affected.

https://t.co/Z1sL8QTZl1

How FedEx is shaving millions from its IT costs

FedEx has saved hundreds of millions of dollars by eliminating costly redundant and legacy technologies, using cloud analytics software to compare the cost and value of IT to the business. For CIO Rob Carter, the path to pare technical debt was paved with some painful discoveries. The journey began in 2009, when Carter realized the shipping giant's application portfolio had ballooned to more than 2,600 applications.

https://t.co/uF91eQTsMd

SA govt's legacy IT management fail

It's a story we've heard time and time again. Government agencies are running legacy, unsupported, and unpatched operating systems. This time the culprit was 10 of South Australia's most critical government agencies, who were outed as having 226 agency servers still on Windows Server 2003 and five servers running Windows Server 2000. The worst offender in the SA auditor-general's report had 71 legacy servers. Executives from that unnamed agency have said they were working to decommission these out-of-date systems, which is certainly a good thing. But some of the operating systems have gone more than six years without a single security patch (Windows Server 2000 went out of support in 2010), meaning these guys have been running high-risk vulnerable servers for over half a decade. In what world is that acceptable?"

https://t.co/6Ap54WtcSK

Hindered by legacy IT systems, Texas CIO forges a way ahead

Over half of the roughly 4,000 business applications in use by the state of Texas are classified as legacy IT systems. CIO Todd Kimbriel has a plan in the works to remedy that.

https://t.co/NwKUfs0mfV

Bridging the gap between security and legacy IT

In June 2016, the U.S. Office of Personnel Management revealed a breach that would potentially impact more than 20 million individuals and was expected to have an impact on national security for years to come. The reason? The legacy systems that stored sensitive personal information weren't capable of the necessary encryption to keep that data safe.

https://t.co/olzFwJCaef

ATMs in Europe remotely mass-hacked to spit out cash

In November, cash machines in at least 14 countries, including the UK and the Netherlands, were remotely hacked by an organised gang to spit out cash for rapid collection by the attackers. An Eastern European hacking group known as Cobalt was identified as the perpetrator. ATMs in Malaysia, Belarus, Armenia, Bulgaria, Estonia, Georgia, Kyrgyzstan, Moldova, Poland, Romania, Russia and Spain were also affected.

https://t.co/obreHUpGiV

San Francisco rail network held to ransom in malware hack

San Francisco's transport agency was hit by a malware hack on November 28th. The hack temporarily allowed commuters to travel for free on the network. Over 2,000 computers belonging to the Municipal Transport Agency (SFMTA), around 25% of the entire network, were infected. The hackers issued a ransom demand of 100 Bitcoin, which equates to around $70,000 (£56,000), for the return of full access to the system.

https://t.co/uBDjQptOjQ

Suspected Hackers Knock German Households Offline

About 900,000 internet customers experienced severe internet outages in late November in what Deutsche Telekom has blamed on an apparent indiscriminate cyberattack. "We believe that influence was exerted on the routers from outside," an unnamed company spokesman told the AFP news agency, noting that malware had been installed on routers that prevented them from connecting to the company's network.

https://t.co/NiCPGHgC7X

Predictive Maintenance and The Industrial Internet Of Things

Back in 2014 an Accenture report predicted that investment in the Industrial Internet of Things would reach $500 billion by 2020. A combination of cheap sensors, powerful data processing and machine learning has enabled companies to make their industrial processes significantly smarter and more efficient. A good example of this in action comes in the rail industry, where fascinating use cases have emerged in the past year.

https://t.co/2bvbvXQmN0

Five Easy Ways to Build Security Into The Internet Of Things

IoT security is at the forefront of everyone's mind these days due to a huge uptick in DDoS attacks coming from our newly connected devices. Here are five things you should do right now to keep you and your company off the list of hacked IoT devices.

https://t.co/bHSncuSmeS

The Internet of Things is making hospitals more vulnerable to hackers

Ransomware and denial of service attacks are just a glimpse of things to come - hospitals are the next big target for cyber-attacks, and the introduction of Internet of Things (IoT) devices make healthcare even more vulnerable. As a result, hospitals need to change their attitude towards security. "The need for improved and even remote patient care drives hospitals to transform by adapting smart solutions, ignoring sometimes the emerging security and safety issues. Nothing comes without a price - hospitals are the next target for cyber-attacks," says European tech security agency Enisa.

https://t.co/CLn7aetuWb

Availability Digest Oldie but Goodie: "Active/Active vs Clusters"

In previous issues of the Availability Digest, we focused heavily on active/active architectures. But there is another, very important high-availability architecture, one, in fact, that is far more mature and predominant than active/active systems, That architecture is clusters. In this article, we describe the cluster architecture and compare it to active/active systems.

https://t.co/cNDUXsK2UN

DMV was unprepared for massive computer meltdown, experts said

The California Department of Motor Vehicles does not appear to have had an adequate disaster-recovery system in place before a computer meltdown wiped out most operations for several days in October. In particular, the DMV should have had a recovery plan that involved distinct computer systems physically separated with independent power supplies. That way, if one data center — or even one section of a data center — overheated or experienced a power surge, backup systems weren't affected. The California DMV ran primary and backup systems side by side in the same hardware cabinet.

https://t.co/nhRit4kA0w

Cloud Inspires Confidence in Disaster Recovery

The cloud is a confidence-booster, in terms of disaster recovery at least. Zetta's recent survey of 403 IT professionals revealed that 90 percent of those who have incorporated the cloud into their disaster recovery setups are confident in their disaster recovery strategy. That figure dips to 74 percent among those who take an on-premises approach.

https://t.co/eUTnZ1yosx

Everest outage was caused by split brains

Server farm Everest"s blackout on 15 November was caused by a power outage combined with stacked routers each running different software versions. A "reason for outage" document issued by Everest admitted to there having been a "loss of connectivity" for clients using IP network services between 0830 and 1030 on 15 November. The trigger of the outage was a power failure, which Everest said it was investigating separately. However, the killer moment happened after techies started trying to restore services.

https://t.co/amlKgf3rmY

Protection of submarine cable infrastructure critical to the digital world

The foundation of today's digital world is based on a network of submarine cables, which carry nearly 100 percent of all electronic communications around the world. These networks connect people and businesses across continents and play an important role in everything we do. Any small disruption to the undersea cable system can potentially interfere with the estimated US $10 trillion worth of transactions that occur globally every single day. When national economies rely heavily on submarine cables, any outage has massive consequences not only for domestic markets but for the entire global economy.

https://t.co/aFy9zvdG7p

How the SSP outage had earthquake repercussions for brokers

It was a summer evening in late August when the lights went out for around 2000 homes in Solihull. The utilities company said it was a faulty end box that caused the outage, and all those affected had power restored by midnight. But that small power outage caused three weeks of chaos for more than 300 brokers, leaving them unable to conduct day-to-day business. Damages ranged from tens of thousands to up to £100,000. One firm is understood to have lost £1.2m from the outage.

http://bit.ly/2hBoWiz

Microsoft still working to fix Outlook sync issues

Beginning Thursday, 17 November, some Outlook customers were unable to access or synchronize their outlook.com accounts while using applications or mobile devices. Six days later, users still were experiencing issues.

https://t.co/nx5vGkfs1F

Westpac Internet banking suffers 'intermittent issues'

Westpac's internet banking, both online and via mobile, has been suspended with "intermittent issues" affecting transactions, balances, and its cardless cash withdrawal function, Get Cash. The Internet and mobile banking issues have been plaguing the bank for several days, with Westpac first commenting on the transaction delays as early as Wednesday, 23 November.

https://t.co/CyKZfOE8Le

Oracle acquires DNS provider Dyn, subject of a massive DDoS attack in October

Oracle recently announced that it has acquired Dyn, the popular DNS provider that was the subject in October of a massive distributed denial of service attack that crippled some of the world's biggest and most popular websites. Oracle plans to add Dyn's DNS solution to its bigger cloud computing platform, which already sells/provides a variety of Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) products and competes against companies like Amazon's AWS.

https://t.co/HcBaWGGf4C

Insurers face same legacy system battle as retail banks

Insurance companies are set to be the next wave of financial firms to accelerate their digital transformation. But like retail banks before them, they face an old foe – decades old legacy IT systems.

https://t.co/fQdySlIEdc

Forget about the cloud: imagine the hybrid multi-cloud fog

The notion that all workloads should run in hyperscale public cloud data centers has a certain appeal but is overly simplistic. An examination of today's digital leaders shows that their infrastructure strategies are substantially more complex. They typically involve a hybrid mix of legacy environments, private and public clouds (as well as the use of colocation facilities and managed services); more than one public cloud at the infrastructure, platform or applications layer; and a spectrum of computing resources ranging from centralized hyperscale cloud data center infrastructure to its polar opposite, the fog, i.e., a highly dispersed edge, being driven by the Internet of Things and a need to enhance user experience.

https://t.co/iU54qLNgiG

Webcam Maker Recalls Devices after Friday's Internet Outage - Information Security Buzz

Chinese electronics firm Xiongmai is initiating a product recall after the enormous hacking attack that took down much of the Internet on the East Coast of the US and also affected Europe on 21 October. The root of the attack was a network of hacked "Internet of Things" devices such as webcams and digital recorders, many of which were made by Xiongmai.

https://t.co/fUCKr4TTRZ

The Internet of Things Leaves Finland Cold

The residents of two apartment buildings in the city of Lappeenranta in Finland found themselves bundling up at home when the heat in the buildings shut down. The reason for the failure wasn't an accident — it was a days-long distributed denial of service (DDoS) attack primarily using Internet of Things devices.

https://t.co/xDHB1SfVzI

Amid major internet outages, downed websites have lessons to learn

Who is to blame for the 21 October attack on managed domain name service Dyn? The elephant in the room is that this probably shouldn't have happened. At the very least, there's a lot to learn already about the frailty of the Internet DNS system and the lack of failsafes and backups for websites and tech companies that rely on outsourced DNS service providers.

http://zd.net/2er2m9l

Massive IoT Hacks Should Lead To Positive Change

Losing access to large parts of the Internet to hackers might feel like the beginning of the end for the Internet of Things. If history is any indication, it's more likely the start of the beginning, the migration to mainstream adoption. It means real standards and more secure devices are coming.

https://t.co/NS5vf6MS6G

Top 9 Cloud Computing Failures

Cloud computing has become a huge market. In a 2016 report, analysts at Gartner predicted that the shift to the cloud will affect more than $1 trillion in IT spending over the next five years. In their rush to participate in this huge market, vendors have been quick to tout cloud successes. Their websites are filled with case studies explaining how various companies have reaped enormous benefits by embracing cloud computing. But what about the cloud failures? Not every cloud deployment has a happy ending. Some cloud computing vendors have made huge missteps, and outages and security incidents have plagued both public and private cloud environments.

https://t.co/4Ksqz9yXJm

Isn't it time the Internet "kill switch" myth died a death?

The famed Internet "kill switch" is a bit of a misnomer, perpetuated because it makes for a good clickbait headline but with little bearing on the real world. The simple truth is that there's no big red button that can bring down the Internet nor any significant part of it. It's one thing for backbone providers to have the ability to shut down all traffic moving through them if needed, and it's quite another for arbitrary threat actors to be able to shut down the Internet via any single "switch."

https://t.co/gzu2UixwMD

Indian CIOs bank on disaster recovery

A recent Ovum/Zerto Asia Pacific Survey interviewed 400 Asia-Pacific enterprises, and the research points at massive growth in the disaster recovery market. “The findings of this report show that no company is immune to a potential outage or disaster; and in the event this does strike, the first few minutes are critical to recovering as quickly as possible,” said Andrew Martin, managing director, Asia-Pacific and Japan, Zerto. CIO India takes a look at what the Indian CIOs are doing to protect their data from IT outages, natural disasters and security breaches.

https://t.co/dY7CF1PF7p

Why Your Backups Are Failing and What to Do About It

Backup and restore failures are an everyday possibility in the world of IT departments. Even though teams have come to expect failure, nobody really enjoys when failure actually occurs. Failures with backup and restore processes generally equate to high costs and the unavoidable loss of data In this article, you will learn about the 5 most common reasons for failure and what you can do about it.

https://t.co/17PaqjpBHV

A Look at New Open Standards to Improve Reliability and Redundancy of Automotive Ethernet

To meet the safety and deterministic latency requirements for controlling a car, a new set of open standards is being developed, collectively referred to as “Time Sensitive Networking,” or TSN. They improve the reliability, timing, redundancy, and failure detection ability of Ethernet to the level where it can be applied throughout an automobile.

https://t.co/e04D6jxOH5

Digest Mng Ed. Bill Highleyman presents "Recent Developments in Improving Mission-Critical System Availability"

Research on making mission-critical systems more reliable continues with some surprising developments. In this talk, we first review the classic theory behind minimizing the probability that both nodes of a HA system will fail simultaneously. We extend this theory by examining nodal failure probability distributions and show that by staggering the nodal starting times so that failure probability distributions are uncorrelated, the probability of a dual node failure and resulting system loss can be greatly reduced. This strategy applies both to hardware failures and to software failures.

https://t.co/pRwe3vntHL

Asda customers unable to pay as card 'fiasco' hits all stores

At the end of October, long queues formed at Asda check-outs after customers across the UK were unable to pay with their cards. Shoppers described the technical issue as a "fiasco" and said it led to "chaos" at supermarkets. The company said all of its 626 UK stores were affected "at one point or another" during the day by the problem with its card payment system.

http://bit.ly/2fz8AF3

From the Availability Digest: High Availability, 1970s Style

In 1972, Digest Managing Editor Dr. Bill Highleyman started MiniData Services, Inc., a payroll processing company. To service MiniData's thousands of customers, Dr. Bill and his team purchased two modern, top-of-the-line minicomputers – PDP-8s from Digital Equipment Corporation. Each PDP-8 had 4K (yes, kilos) of memory, and each system processed different payrolls. Additional 4K memory banks could be added. If one PDP-8 failed (and the MiniData PDP-8s never did), the company was confident that they could move the customers off the failed system and could process all the payrolls on the surviving system. Back in the day, such confidence was all that constituted the concept of high availability. There was no data replication and no active/backup or active/active configurations. "High Availability, 1970s Style" is Dr. Bill's own account of how his MiniData team operated a successful payroll company with mere kilos of memory, no operating system, and software developed in-house.

http://bit.ly/2f69mdu

Liberia calls for international assistance after crippling cyberattack

Authorities in Liberia are seeking the assistance of the US and UK governments to help them secure their Internet infrastructure following a crippling cyberattack that brought down 60 percent of the country's network. The size of the attack against Liberia is cause for alarm, according to Eugene Nagbe, the country's information minister, who believes Liberia was targeted by hackers because its network was perceived as being weak.

https://t.co/WUi4CwIQdY

Adelaide hospitals hampered by nine-hour system outage

South Australia's health department is investigating what caused a nine-hour outage to its notorious EPAS system across three major Adelaide hospitals on 7 November.Between 3pm and midnight Adelaide time, the critical medical records system became unusable or completely unavailable at the Queen Elizabeth Hospital, the Repat Hospital, and the Noarlunga Hospital. The three sites are the first to be hooked up to the electronic patient administration system (EPAS).

https://t.co/34dJ6wyHSf

Whistleblower: Fairview Health Services' IT system keeps crashing

In the fall of 2015, Fairview installed a new storage system. Hitachi's successor, EMC, a company owned by the multinational corporation Dell, supposedly would be a state-of-the-art replacement. But the Dell EMC system is having stubborn problems that are affecting other crucial IT components.

https://t.co/vWz0Vk4alA