

the Availability Digest™

Volume 12
Issue 6

--- achieving 100% uptime

June 2017

The digest of current topics on Continuous Availability. More than Business Continuity Planning.

BCP tells you how to **recover** from the effects of downtime.

CA tells you how to **avoid** the effects of downtime.

www.availabilitydigest.com

Follow us



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

Technical
Writing

The articles you read in the Availability Digest result from years of experience in researching and writing a variety of technical documents and marketing content. It's what we do best, and we provide our services to others who value high-quality content created by IT specialists. [Ask us](#) about

- articles
- white papers
- case studies
- web content
- manuals
- specifications
- patent disclosures

In this issue:

[Never Again](#)

[British Airways Downed by Fat Finger](#)
[WannaCry Ransomware Global Attack](#)

[Availability Topics](#)

[Fog Computing Improves App Availability](#)

[Product Reviews](#)

[Carbonite – The Online File Copy Utility](#)

[Tweets](#)

[The Twitter Feed of Outages](#)

Browse through our [useful links](#).

See our [article archive](#) for complete articles.

Sign up for your [free subscription](#).

Visit our [Continuous Availability Forum](#).

Check out our [seminars](#).

Check out our [technical writing services](#).

Watch Out For Fat Fingers

I recently presented a seminar on system outages caused by fat fingers. I defined these as improper or erroneous commands entered by IT staff that caused a system to malfunction. For instance, Amazon wanted to redirect traffic from one of its 42 Availability Zones so that it could increase the capacity of that zone. Instead of rerouting traffic to an alternate high-capacity network, it rerouted traffic to a slower secondary network, taking down the Availability Zone for four days.

In this issue, we describe another fat-finger error. A maintenance technician erroneously turned off the UPS unit in a British Airways data center and caused significant disruption of BA's services. Over 1,000 flights were canceled on that fateful weekend.

Fat finger errors can be eliminated by employing human redundancy. For critical commands, one person enters the command and another checks it before it is executed. Why doesn't anybody do this?

These articles are an example of the stories we write for the Digest and for others. If you have an article, a case study, or a white paper that you would like written, come talk to us. We also provide consulting services and seminars on high- and continuous availability. We will be glad to help you.

Dr. Bill Highleyman, Managing Editor

Never Again

British Airways Downed by Fat Finger and Testing Shortsightedness

A worldwide systems crash in a British Airways (BA) data center caused significant disruption and flight cancellations on Saturday, May 27, 2017. All flights from Heathrow and Gatwick were canceled on Saturday. Dozens more were cancelled on Sunday. More than 1,000 flights were cancelled at 170 airports in 70 countries.

The outage was caused by human error. A technician mistakenly turned off the UPS system in BA's active data center, shutting down all of BA's servers. Power then was restored in an uncontrolled manner, physically damaging many of BA's servers, storage units, and communication systems. It took the weekend for BA to repair its equipment and restore service.

Unfortunately, BA suffered from a syndrome that we see faced by many organizations. BA had never fully tested its failover capabilities to its backup data center. One of the best plans I have seen to test failover is by a company that performs a full failover every three months. It then runs on that system for three months and repeats the failover to the original system. Since each system is running production for three months at a time, there is a high degree of confidence that each system is operating properly and that failovers will succeed.

[--more--](#)

WannaCry Ransomware Global Attack

WannaCry is ransomware malware. If it infects your computer, it encrypts all your files and demands a ransom in order to get your files decrypted.

Fortunately, I escaped unaffected. I had updated my Windows operating system to Windows 10, a level that WannaCry could not infect. Furthermore, I back up my files in real time with an online service that would have allowed me to recover from a WannaCry infection.

WannaCry appears to have run its course. However, there is no assurance that it will not return or that other ransomware attacks will occur. It is therefore imperative that you keep backup copies of all of your files so that you can restore them in the event of an attack. I highly recommend using an automatic online copying service such as Carbonite to perform this task for you.

It is unknown who launched the attack. However, Symantic has identified the tools used by WannaCry as the same tools used by the Lazarus Group. This organization carried out the 2014 attack on Sony after Sony released its film "The Interview" about an assassination attempt on the leader of North Korea. The Lazarus Group is linked to North Korea.

[--more--](#)

Availability Topics

Fog Computing Improves Application Availability

Fog computing is a decentralized computing architecture in which applications and the data they process are distributed in the most efficient places between the data source and the cloud. Fog computing extends the services provided by the cloud to the edge of the network via 'cloudlets', bringing the advantages and power of the cloud closer to where the data is created. Fog computing allows data to be accessed more efficiently and processed more rapidly and reliably from its most logical location.

Equally important is the increase in availability that fog computing brings to applications. Should the cloud fail, an event that normally would bring down the applications, the distributed nature of fog computing can allow the critical aspects of application processing to continue via the cloudlets with little impediment.

Fog computing reduces the bandwidth required by classic cloud computing because it preprocesses device data at the source and sends only critical data to the cloud. In addition, fog computing offers a degree of protection from cloud failures since critical tasks still can be carried out by the cloudlets.

[--more--](#)

Product Reviews

Carbonite – The Online File Copy Utility

In my article in this issue of the *Availability Digest*, "WannaCry Ransomware Global Attack," I described how I would have been protected if my system had been attacked by the WannaCry ransomware. It installs itself on a system and encrypts all of the system's files. It then posts a message demanding a ransom.

I was protected from WannaCry in two ways. WannaCry infected mainly Windows 7 servers. I already had upgraded to Windows 10, which was protected from WannaCry infections.

The other protection was that my files were all backed up online. If WannaCry had infected my system and encrypted my files, all I would have had to do was to scrub those files from my system and reload them from my online backup. The online copy service I use is Carbonite.

Carbonite comes at a price of \$59.99 per year. In my view and experience, this is an expense well worth it. There are other online file copy utilities available. You are well advised to choose one of these utilities and use it to provide security for your file system. Someday you are likely to say, as I have done, "God bless xxx."

[--more--](#)

Tweets

@availabilitydig – The Twitter Feed of Outages

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.

Now with our Twitter presence, we don't have to feel guilty. This article highlights some of the @availabilitydig tweets that made headlines in recent days.

[--more--](#)

Sign up for your free subscription at <http://www.availabilitydigest.com/signups.htm>

Would You Like to Sign Up for the Free Digest by Fax?

Simply print out the following form, fill it in, and fax it to:

Availability Digest

+1 908 459 5543

Name: _____

Email Address: _____

Company: _____

Title: _____

Telephone No.: _____

Address: _____

The Availability Digest is published monthly. It may be distributed freely. Please pass it on to an associate.

Managing Editor - Dr. Bill Highleyman editor@availabilitydigest.com.

© 2014 Sombers Associates, Inc., and W. H. Highleyman