the Availability Digest™

Volume 7
Issue10

--- achieving 100% uptime

October 2012

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

Thanks to This Month's Availability Digest Sponsor

This free newsletter covers what's new and exciting in the HP NonStop world.
Tandemworld is the premier network for all Tandem/HP NonStop resources.
Tandemworld provides permanent or contract specialists for NonStop, UNIX, IBM and other systems.

In this issue:

Browse through our Useful Links.

Check our article archive for complete articles.

Sign up for your free subscription.

Join us on our Continuous Availability Forum.

Check out our seminars.

Check out our technical writing services.

Security Starts Abroad

Hardware failures and human errors are not the only things that can take down a system. We are now beginning to see devastating attacks, often sponsored by foreign agencies and governments, that have caused major harm to institutions. It is our side against their side.

We are not always the innocent ones. It is generally conceded that the Stuxnet virus that sped up and damaged Iran's centrifuges was the work of the Israeli and U.S. governments (see our article entitled "Stuxnet – The World's First Cyberweapon" in our March 2011 issue).

Just this last month, a hacktivist group believed to be an arm of Hamas and sponsored by Iran launched a massive Distributed Denial of Service (DDoS) attack that took down the online banking services of several major U.S. banks for a day in retaliation for the YouTube video "Innocence of Islam" (see this issue's article entitled "Islamic Hactivists Attack U.S. Banks").

These threats are so sophisticated that it may be difficult to defend ourselves against them. However, we must be aware of their presence and have plans to continue providing our products and services if our systems should be crippled by such an attack.

Dr. Bill Highleyman, Managing Editor

Never Again

Islamic Hacktivists Attack U.S. Banks

The posting of the fourteen-minute anti-Islamic trailer “Innocence of Muslims” on YouTube in early September, 2012, did more than spark outrage and massive anti-American demonstrations against U.S. embassies throughout the Arab world. It launched cyberattacks against the largest American banks in retaliation for the film. Massive Distributed Denial of Service (DDoS) attacks took down the web sites of Bank of America, JPMorgan Chase, Wells Fargo, U.S. Bank, and PNC for a day each over a two-week period.

The hackers vowed to continue the attacks until the “nasty movie” was removed from the Internet.

However, the demand of the Izz ad-Din al-Qassam Cyber Warriors to “erase the nasty movie” has not yet been met. Google, the owner of YouTube, has removed the movie only in countries that have laws against such blasphemy. Where freedom of speech is guaranteed, such as in the U.S., the movie is still available online. However, other countries have blocked YouTube until the video is removed.

On September 27, 2012, U.S. federal authorities arrested Nakoula Basseley Nakoula, who created the movie under the alias “Sam Bacile.” He was charged with parole violations and is being held without bail.

--more--

Best Practices

ISO 22301 – The New Business Continuity Management Standard

ISO 22301, issued on May 15, 2012, is the first international standard for Business Continuity Management (BCM). It builds on the British Standards Institution’s BS 25992-2 standard, which has been widely accepted outside of the UK. It is a relatively brief specification, taking only fifteen pages exclusive of definitions and bibliography.

Our modern just-in-time business processes would not be possible without interconnected IT systems and interconnected organizations. A disruption somewhere in this supply chain can have a ripple effect throughout the society in which the disrupted process or system is a part. Natural and man-made disasters will happen. We cannot always avert them. But we can anticipate them and can take steps to prevent the cascading of the consequences that often follow. This is the thrust of ISO 22301.

ISO 22301 is just the first business continuity specification to be issued by ISO. Coming soon are ISO 22313 – Business Continuity Management Systems - Guidance and ISO 22390 – Guidelines for Exercises and Testing.

--more--

Is Preventive Maintenance Preventive?

Our Never Again articles are rife with major outages that have been caused by poorly performed maintenance. A recent 24x7 Exchange conference focused on preventive maintenance.

Corrective maintenance is mandatory. Preventive maintenance is optional. All maintenance can cause outages. It is estimated that 70% of all IT outages have been aggravated by human actions. Maintenance errors dominate these outages. Preventive maintenance procedures must be carefully controlled so that an action that is supposed to improve data center availability does not instead take it down.

We invest a lot of money in our data centers to make them redundant so that any single failure can be tolerated. Why not do the same for the 70% problem - humans? If there is a critical operation that must be performed for maintenance, whether corrective or preventive, provide human redundancy. Use two people, one to define the action to be taken and one to confirm it.

So far as preventive maintenance is concerned, it seems that the consensus is that a little goes a long way. Just don't overdo it.

--more--

Availability Topics

FS-ISAC: Financial Services – Information Sharing & Analysis Center

FS-ISAC, the Financial Services – Information Sharing & Analysis Center, is an industry forum for sharing critical security threats facing the financial services industry. FS-ISAC members receive timely notification and authoritative information for protecting their critical systems from physical and cyber attacks.

FS-ISAC is owned by its 4,000 members. Members voluntarily and anonymously submit information to the FS-ISAC database for authentication and analysis. As information is received, it is verified; and the threat level is analyzed. Recommended actions are disseminated to the FS-ISAC membership via FS-ISAC's Critical Infrastructure Notification System (CINS), run by VeriSign.

FS-ISAC manages scheduled calls for members to coordinate information. It runs multiday spring and fall annual conferences and sponsors weekly webinars on a variety of security issues. It also publishes a monthly newsletter.

FS-ISAC has been operating out of the public view for over a decade protecting our financial services industry. It played a particularly important role in the recent DDoS attacks that disabled for a day the online banking portals for many major banks, including Bank of America, JPMorgan Chase, U.S. Bank, Wells Fargo, PNC Bank, Capital One, SunTrust Bank, and Regions Financial.

--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.
© 2012 Sombers Associates, Inc., and W. H. Highleyman