

TEST DATE: 5/18/2010-5/20/2010

Revision 6/11/2010



## 2010 DISASTER RECOVERY TEST REPORT AND GAP ANALYSIS

The annual disaster recovery test was conducted 5/18-5/20, 2010 at the IBM Schaumburg BCRS facility. This test sets a new watermark for the CU\*Asterisk network in our disaster recovery and business continuity efforts as it represents the introduction of the new Muskegon, Michigan, data center into the test's scope.

Muskegon allows for an entirely new way of thinking about our disaster recovery and business continuity planning and will challenge traditional DR/BC paradigms. We need to start planning our networks and systems deployments in a new way and challenge what features and services are and are not critical to our business.

There is no doubt ItsMe247.com has become a cornerstone of our network and it was time to step up and move this service into a Tier1 recovery level equal with that of the host system. Lately we've challenged what belongs in Tier1, and we will continue to do so every year as we evaluate our network's products and services. A few years ago, we moved our third party relationships into Tier1 and started an aggressive annual testing schedule. We've also begun adding redundancy to third parties at our 28<sup>th</sup> Street facility. We will continue to evaluate and expect that Tier1 will continue to evolve as driven by business requirements and risk analysis.

This event tested our ability to operate ItsMe247.com from Muskegon connected to a host recovered inside of IBM's BCRS network. This is a significant event because for ItsMe to function properly for the member, it has to have roughly equivalent capacity to the production web site. So we layered in load balancing, redundant web servers, and following our HA system strategy, a database server identical to production.

At the IBM BCRS facility we recovered the host and established a VPN connection to Muskegon so the ItsMe servers could communicate securely with the host. Testing of ItsMe247 involved test participants at the BCRS facility and back in Grand Rapids accessing their accounts and performing money transactions. Because we did not want to create issues with members performing transactions against the recovered host, general member traffic was not allowed to connect to the site.

The ItsMe247.com network in Muskegon is one that remains in place permanently so as to be ready for an event with the production network or Kentwood datacenter. Next steps beyond this disaster recovery test are to perform actual member-facing testing in which we'll redirect ItsMe247.com traffic from the main site to the Muskegon facility.

This test also represents the first time ACH returns through the FRB were tested from the disaster recovery site using the BTCU buddy-bank system (ACH had previously been successfully tested.)

These tests are beneficial on many levels. They allow us to verify our procedures, identify gaps in them to be adjusted, and continue pushing our capabilities forward, expanding our expertise and abilities. This year we took the largest ever crew, which allowed opportunities to cross-train on procedures and expand the knowledge across team members. There were hiccups, as there always are, which are identified in the following GAP ANALYSIS section. These will be addressed in updated process and procedures.

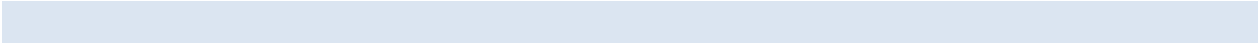
Please pay close attention to the comments in the FUTURE RECOMMENDATIONS, particularly comments #1 and #6. Based on projected conversions and growth, we should consider an upwards adjustment to the hard drive capacity contracted in our IBM BCRS agreement, due for renegotiation this October. Look for a recommendation from Todd Wolcott soon. Finally, in #6 the network team is challenged with finding a different way to handle third party communications recovery for the future. Third party recovery is always tricky because each one does it differently and we're not in control of the design or implementation. A plan permanently installing communications in Muskegon, backing up 44<sup>th</sup>, and backhauled to IBM BCRS will provide a stable, secure, redundant environment that will not necessitate dragging equipment back and forth. It should also allow us to eliminate ISDN circuits from our contract and save some money. Look for a plan later this summer.

## GAP ANALYSIS

1. File XXE was not present for two recently converted credit unions – Edco and Des Moines and had to be created manually. Procedures should be modified to account for these necessary empty files needed for recent credit unions during the recovery efforts.
2. Linoma keys used in production are the original keys from 2008. They had not been upgraded as thought to the 2009 keys. This prevented recovery of the encrypted card file data until key material was moved over from PROD in Grand Rapids. It should be noted we still have the 2008 key material in both our off-site secure storage locations, and the data could have been recovered with the use of this material. Linoma had published somewhat contradictory instructions for replacing production keys and it was thought the 2009 keys were in use when they were not. New procedures have been established, documented, and tested for putting new key material into place. The 2008 keys have all been updated to the 2009 keys on all systems.
3. The VPN to FiServ wouldn't initially come up properly. The NAT rule was restricted to IKE, but didn't include ESP. ESP was added, but didn't fix the VPN. Disabling VPN termination on the FW allowed the tunnel to come up, but disabled the MKG VPN.
  - a. Reconfiguration of the FW allowed both VPN connections to be active. By changing to a NAT any (from only NAT'ing IPSec ports) and restricting access via the FW policy we were able to get both VPNs up.
4. Shazaam could not access their router because they did not have logon information. They asked us to perform a password recovery, which we did. We examined the router config to see if it could handle NAT translation for the VPN termination as the third party network at IBM uses private IP addresses. Their configuration would not handle NAT-T so we created a new DMZ interface on the firewall in transparent mode with the WAN and used an available public IP address for the router. However, the VPN would not come up, nor would the SSH server, likely due to an IOS software bug. Shazaam decided to overnight a router to us at IBM and Shazaam was tested successfully.
5. We didn't test FTP file transfers with FiServ. The connection was up and working, but they were not ready for us to do an FTP test as their application folks were not prepared. We rescheduled for the next day but wound up cancelling as FiServ needed to make additional VPN reconfigurations and we decided to skip due to time. We had already validated the communications end to end inclusive of the application layer. The FTP test at that point is simply icing on the cake.
6. The static IP addresses assigned to us by IBM BCRS did not work initially. IBM determined that although their design called for our Internet connectivity to be backhauled out of Boulder, the static IP addresses in our contract must be backhauled from Sterling. Once IBM staff determined the error,

they were able to route us out of Sterling and provide us with our contracted IP's. This delayed bringing up the VPNs.

7. The 400FTP DR server had a dead CMOS battery. This was bypassed at boot. However, the server is of the age (rebuilt GUAPPLE) where it should be replaced prior to next year's test. An amount should be reserved in the 2011 budget.
8. The Statement Company DR IP is configured as a secondary peer and in order to roll over to the DR site the primary VPN needs to be disabled. This may cause service interruptions during test activities and should be noted in test documentation.
9. New file XXOPS library on PROD was not saved and didn't come over to DR. This is by design. These libraries need to be recreated at DR – modify build sheets.
10. Take the edit out for a tape drive for the option to rebuild end of day, beginning of day save files. Tape not needed.
11. Add building of archive libraries (not replicated or backed up – temp) as step in CU\*BASE restore.
12. Update recovery doc to put jobs on hold if ROBOT subsystem is started up – hold scheduled jobs.
  - a. Data was accidentally sent to Vacationland's InBusiness 360-view production server, which rejected the file because of a date miss-match. The process should be updated to prevent accidental transmissions.
13. Change host IP in our subsystem for 5/3<sup>rd</sup> so as not to accidentally connect with their production during a DR test



## FUTURE RECOMMENDATIONS

1. All Libraries were recovered on the DR system and approximately 1.32 TB of data was used with BOD and EOD files present. We currently contract 1.5 TB of disk space. Contracted space allocation should be considered during renegotiation with IBM BCRS. The contract expires 10/2010 and projected adjusted numbers should be available by 7/1/2010 for the annual budget recast.
2. Need to verify contracted Internet bandwidth as we seem to be getting around 6 Mbps down and only about 600 Kbps up.
3. A new process should be considered to deal with multiple automated programs that attempt to FTP files to the HA host, which is not present in a disaster situation. It could potentially complicate testing efforts if the recovered host were ever able to successfully copy a file to the HA machine in Grand Rapids. Currently these are handled individually with programmers or operators aborting transmissions that will never connect. This wastes time and system resources.
4. Acquire a new 400FTP test server to replace the DR test unit which is reaching end of hardware useful life. The new system should be located in Muskegon and kept in a ready state. Future tests should be performed from Muskegon, and we should no longer be physically transporting the box for testing purposes.
5. The LAN network at IBM BCRS should be adjusted to allow both PCs and Laptops to be available in the same cube (both network ports need to be active.) This is a testing environment change to provide for improved efficiencies for the recovery team.
6. We recommend an updated plan for testing third parties that does not involve moving gear from site to site and asking them to reconfigure for the test. Third parties are becoming increasingly resistant to reconfiguring their equipment for our test activities and further are confused by the production/HA/DR site designation. Internal Networks will draft a plan to backhaul third parties from a central location via MPLS or VPN to IBM BCRS that will allow the third parties to leave equipment configured statically and in place (likely from Muskegon). This plan, if adopted by CU\*Answers, would represent a new standard for third party communications moving forward beyond 2010.