CU*ANSWERS - 2014 DISASTER RECOVERY TEST GAP ANALYSIS JUNE 12, 2014

OVERVIEW

The annual CU*Answers' Disaster Recovery Test was conducted on 5/20-5/22, 2014 at the IBM BCRS (Business Continuity and Resiliency Services) hot-site facility in Sterling Forest, NY. The test incorporated the successful restoration of our core processing CU*BASE/GOLD production host and network environment including "proxy" credit union verification over MPLS and VPN networks. This report highlights the key changes implemented for the 2014 recovery test to increase the scope and complexity, identifies any problems that surfaced requiring troubleshooting and/or procedural changes, and provides recommendations for improving the effectiveness of the CU*Answers' Disaster Recovery program.

As in the previous two years, recovery teams were divided among the IBM hot-site facility and the CU*Answers secondary (HA) datacenter in Muskegon, MI. Recovery team members at the secondary datacenter accessed the recovered IBM host utilizing remote access tools. By dividing the staff among facilities, we were once again able to rotate in additional team members for the purpose of gaining experience and knowledge in recovery procedures while operating in multiple shifts throughout the 60-hour event.

The outline of the recovery event is shown below. At each step, multiple tests and audits are performed to ensure system and data accuracy:

The first 24 hours of the test included the following activities:

- IBM host operating system installed and configured
- Network and USER security configured
- CU*BASE/GOLD environment and applications restored
- Credit union libraries and objects restored

The next 24 hours of the test included the following activities:

- Daily operational tasks confirmed concluding with full EOD/BOD system processing
- Core applications tested including ItsMe247 (online banking)
- Secure file transmissions using redundant GOAnywhere and 400FTP servers performed
- CU*BASE/GOLD availability and data verification testing by proxy credit union sites confirmed

The remaining 12 hours concluded the test with:

- Any pending issues that surfaced during the test were resolved or identified for new projects
- Test completion and remote host sanitation (full data wipe)
- Full test debriefing by Recovery Teams held to document required changes to plans and procedures
- Meeting and event notes gathered for inclusion in draft and final publication of the gap analysis report

APPRECIATION FOR PARTICIPANTS

In addition to all of the internal staff members representing multiple recovery teams trained for specific roles and responsibilities during the recovery process, we would like to extend a special "thank you" to the following clients and vendors for their participation in this year's successful disaster recovery test:

- **Besser Credit Union**
  - *(Proxy credit union)*
- **Focus Credit Union**
  - *(Proxy credit union, FEP Beta client)*
- **SAGE Direct**
  - *(Member credit card and end-of-month statement processing)*

FIRST RECOVERY TEST PERFORMED DURING A HIGH-AVAILABILITY (HA) ROLLOVER EVENT

Just 48 hours prior to the start of the 2014 disaster recovery test, an emergency HA rollover was performed, redirecting core-processing production traffic to redundant systems at the secondary datacenter (the same location where recovery teams members would be assembling for the annual test). This meant that all of the planning and preparation invested in the 2014 recovery test had to be revisited and revised due to the fact that 'live' production traffic would now be traversing the secondary datacenter network along with 'test' traffic. To ensure there was no blending of live and test data, certain at-risk portions of this recovery test were identified and scaled back or omitted altogether.

One of the tests omitted included transaction posting with select third party EFT vendors. Since the secondary datacenter was at the time acting as the "production center", making the necessary changes to enable connectivity from the vendor to the restored host in Sterling Forest could potentially have cause service disruptions to 'live' EFT transactions. To enhance network availability for third-party EFT vendor communications, CU*Answers has initiated a project with each vendor beginning in 2014 to add redundant communications at the secondary HA datacenter that will enable us to redirect live production traffic, reducing or eliminating the need to configure stand-alone third-party environments for the purpose of the annual recovery test.

To add another layer of complexity to the 2014 recovery test, the media tapes required for the restoration process in Sterling Forest contained the same data from the actual day of the emergency HA rollover. To accomplish this, recovery team members had to transport the tapes from the primary to the secondary datacenter to back up the (now active) HA host, travel to the Grand Rapids International Airport, board a plane for Sterling Forest, and deliver the tapes for the restoration; all within a 28 hour period.

As introduced for the 2013 recovery test, a security control was implemented to restrict command-line access for recovery team members. In its place, a TOOLBOX menu (command-line replacement app) was utilized, as is standard in the production environment. As an additional security measure, recovery team USER profiles on all CU*BASE/GOLD "production hosts" had been disabled for the duration of the 2014 recovery test.

SAGE DIRECT STATEMENT TRANSMISSION TEST

For the purpose of the 2014 test, recovery teams were able to generate and securely transmit encrypted statement files from our recovered host in Sterling Forest to the redundant FTP server at our secondary (HA) datacenter, and then on to the production host at SAGE Direct's main office location for processing. The test was stopped at the point SAGE systems were able to decrypt and format the data for printing. For the purpose of the 2014 test, there was no need to print the statements with "test" data since the SAGE production facility was already actively printing statements with live data.

For the 2013 recovery test, these completed files were then transmitted securely to SAGE Direct's alternate print provider (Presort Services) for printing and mailing. A CU*Answers recovery team member was on hand to witness the file reception, processing, and printing to confirm the vendor's ability to provide critical services in the event of a disaster. This extended portion of the process at the alternate print provider site will be considered in the scope of the 2015 recovery test.

AUTOMATED CLEARING HOUSE TRANSMISSIONS

Multiple alternate options are available during a scenario in which the transmission of ACH files through our production datacenter is prohibited due to a service disruption or disaster. The preferred option is the utilization of a redundant FedLine VPN connection through our secondary (HA) datacenter. This redundant VPN option is tested multiple times each year during our HA "rollover" exercises. An alternate option is the use of the FRB "Buddy Bank" partnership with Honor Credit Union.

For the purpose of the 2014 test, recovery teams had planned to send and receive "test" files using the redundant FedLine VPN at the secondary datacenter. Given that for the duration of the test, the secondary datacenter was the acting production site actively using the redundant FRB VPN, sending and receiving "test" files was not considered necessary to confirm connectivity.

ITSME247 APPLICATION TESTING

Also included in the annual recovery test is the availability and functionality of the ItsMe247 (including mobile banking) and ItsMyBiz applications hosted on the redundant stand-by server pool at the secondary (HA) datacenter retrieving data from the recovered host in Sterling Forest. During the 2014 test, internal and remote users were able to point their browsers to the recovered site, authenticate, and check application features. For this test, servers hosting OBC (Online Banking Community) were not included, taking the users directly to the login prompt.

With the cooperation of the CU*Answers ASP Programming Team, features of the mobile banking suite were tested successfully.

RECOVERING AND TESTING MULTIPLE CONCURRENT VERSIONS OF CU*BASE/GOLD

The rapid pace of new application revisions requires careful planning of data archiving strategies to ensure that recovery timelines can be met under unexpected circumstances. This includes system, application, and member data in a rotation mix of monthly, weekly, twice daily (EOD/BOD), using a combination of full, incremental and differential strategies to optimize available time and resources. Encrypted media tapes are then rotated between off-site secure storage facilities to ensure availability should a recovery incident occur.

To maximize the 60-hour window opportunity for the 2014 recovery test, a portion of the encrypted tapes required for the system restoration were shipped to Sterling Forest (on 5/16/2014) ahead of the designated recovery team members for loading at 00:00. The most current daily tapes (from 5/19/2014) travel with the recovery team to the restoration site for arrival at 08:00. This tape travel time combined with regular production software updates means that the potential for application and configuration changes between data restored on the test host and production data may not match at the time of the test. This can present problems (as was the case in the 2013 test) during “proxy” credit union testing when participants are operating with different software versions. The 2013 test resulted in procedural changes to the recovery process and confirmed during the 2014 test.

To validate these procedural changes, “proxy” credit unions were intentionally selected representing both the standard and the FEP (beta) CU*BASE/GOLD versions. In each case, tests were successful with no problems reported. Although the amount of data restored has grown considerably since the last recovery test, restoration times were not lengthened, due in part to the recent hardware upgrade to LTO-5 tape technology.

GAP ANALYSIS

The remainder of this report highlights the issues noted and lessons learned as well as recommendations for changes to existing operations and/or future testing.

ISSUES NOTED AND LESSONS LEARNED

1. Coordinating these annual 60-hour recovery windows between multiple recovery teams, vendors, and proxy credit unions requires scheduling resources in advance. Between the time the hot-site location was reserved and the recovery test performed, we had upgraded the tape drive technology used at both the primary and secondary datacenters. It was during an 11th hour double-check prior to the recovery test where it was discovered that the hot-site resources reserved included media tape drives that were not compatible with our production tapes.

    a. Working with IBM BCRS, we were able to make the necessary hot-site corrections before the first set of tapes arrived for restoration, averting any delays.

    b. More frequent checks will be carried out moving forward to confirm hot-site resource compatibility and consideration of the effect on recovery testing during any hardware/software upgrades will be added to existing project sheets.

2. Early in the recovery test window it was discovered that network administrators were unable to authenticate on the DR firewall in Sterling Forest, NY (although the firewall appliance was functioning normally otherwise).

    a. To remedy this, the firewall appliance was manually restarted by a recovery team member between restoration procedures (to prevent any potential interruptions).

3. iSeries Administrators were unable to access IBM remote console network following the initial system load.

    a. This problem was due to the browser proxy configuration on the LAN at the secondary datacenter. Once corrected the problem was resolved and access was made available.

4. During the restoration process, some procedures (while automated in production) were disabled to prevent any potential interruptions to production core-processing (i.e. notification, etc.). These procedures were performed manually for the purpose of the test. This created some instances where certain modules required reinstallation if not installed in the sequence expected by the system.

    a. One example of this was related to launching Client Access sessions. After troubleshooting error messages with IBM support, the decision was made to revert back on the procedures list and reinstall the required modules. This corrected the problem.

5. Mid-way through the system and library file restoration process, system hardware error messages began to appear on the host in Sterling Forest, indicating a failing (redundant) power supply and a failing disk in a RAID array.

    a. IBM support was engaged to troubleshoot and correct the error messages. Knowing that the failure of the single active power supply or another disk in the array could potentially cause us to start the recovery process over, the decision was made to continue. The single active power supply did function properly throughout the test. During the restoration, IBM support replaced the failed disk drive. This did produce some I/O degradation during the RAID array rebuild but by the conclusion of the test, no measurable delays were experienced.

FUTURE RECOMMENDATIONS

Over the past few years, the amount of planning and resources required by the annual disaster recovery test just to make sure that there are no interruptions to the production environment has nearly exceeded that required to perform the test itself. It’s almost to the point where it’s costing us more (at least in preparation time) to prevent us from creating a disaster during the test than to practice recovering from one. This was never more evident than during the 2014 recovery test that happened to fall during a week where an emergency HA rollover was required.

This is not to say that the benefits gained from the 2014 test were any less. While a fewer number of tests were performed compared to previous recovery tests, more knowledge and awareness was gained regarding the complexity and dependencies (internal and external) required by the production system and vast network environment. The rigorous process of planning how “not” to break systems and applications gives a fresh perspective as we consider those scenarios that could potentially create the undesired effect with proper controls and procedures to prevent it from occurring.

Another feature that is very efficient in the production environment but inhibits our ability to perform recovery tests the way we have in the past involves the increasing number of automated processes and procedures, especially during system start-up. In an effort to control the (unintended) effects of specific scheduled automated tasks (notifications, etc.) during the recovery process, many of the automated tasks are suspended. As more and more tasks become dependent on one another, problems arise during the restoration process when performed manually. In an actual disaster scenario, these automated tasks would not be suspended (with no fear of intruding on the production environment). This is another example of investing more time trying “not” to break something than trying to restore it.

As the CU*Answers High Availability and Disaster Recovery programs continue to develop, the significance of continuing operations and navigating through potential disruptions using HA technologies and risk mitigating controls (i.e. redundancy, replication, etc.) is growing in significance over technologies and procedures to recover. To be effective, future tests should reflect this with an increasing scope during HA rollover exercises (incorporating redundant vendor networks, etc.) and a narrowing scope for DR tests (more focused on host bare-metal restoration in a controlled environment, etc.).

Recovery teams will be working with Senior Management in the coming months to revisit the goals and objectives of the High Availability and Disaster Recovery programs to design tests and exercises that are most effective and aligned with the business objectives of the organization.

Report submitted by: Jim Lawrence, CBCP | CU*Answers | Manager of Disaster Recovery and Business Resumption Services