CU*ANSWERS - 2013 DISASTER RECOVERY TEST GAP ANALYSIS MAY 17, 2013

OVERVIEW

The annual CU*Answers' Disaster Recovery Test was conducted on 5/7-5/9, 2013 at the IBM BCRS (Business Continuity and Recovery Services) hot-site facility in Sterling Forest, NY. The test incorporated the successful recovery of our core processing (CU*BASE/GOLD) production host and network, multiple third parties including ATM/Debit transactions, Credit Card and member statement processing , and "proxy" credit union verification over MPLS and VPN networks. This report highlights the key changes implemented for this test to increase the scope and complexity, identifies issues that surfaced requiring troubleshooting and/or procedural changes, and provides recommendations for improving the effectiveness of our disaster recovery program.

For the second year in a row, 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 via remote access tools. By dividing the staff, we were once again able to rotate additional (new) team members 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
- Daily operational tasks confirmed concluding with full EOD/BOD system processing

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

- Application testing including ItsMe247 (online banking) performed
- Connectivity and transaction testing with proxy third party vendors completed
- 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 are resolved or identified for new projects
- Test completion and remote host sanitation (full data wipe)
- Full test debriefing by Recovery Teams to document required changes to plans and procedures
- Gap analysis report generated and submitted

APPRECIATION FOR PARTICIPANTS

In addition to the internal staff members who are trained for specific roles and responsibilities for the CU*Answers Recover Teams, 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:

- **State Transportation Employees Credit Union**
    - *(Proxy credit union)*
- **Lake Huron Credit Union**
    - *(Proxy credit union)*
- **Honor Credit Union**
    - *(ACH "Buddy Bank" partner)*
- **SAGE Direct**
    - *(Member credit card and end-of-month statement processing)*
- **Vantiv (ISOFTH)**
    - *(Third party transactions)*
- **Federal Reserve Bank**
    - *(ACH file transmissions)*

IMPROVED COORDINATION OF FUTURE TESTS AND EXERCISES

For an "ideal" recovery test, the element of surprise contributes to the true measure of an organization's ability to recover within an acceptable timeframe. For the purpose of our recovery tests, we require the participation of multiple vendors and clients, all within a 60-hour windows, reserved months in advance. To maximize this limited opportunity, careful pre-planning and coordination is required. In past tests, this was performed in a decentralized manner, with each recovery team coordinating tests with their respective vendors and clients. With the increasing complexity and scope of tests being performed each year, the need for improved coordination became very evident during the 2013 recovery test.

For all recovery tests and exercises moving forward, communication and coordination with external vendors and clients will be performed by the event coordinator (Business Resumption Manager). This will include the selection of participating vendors and clients based on the determined business objectives of each recovery test.

In addition, future tests will be designed and orchestrated with a progressive degree of difficulty to strengthen our procedures and problem solving skills.

ENHANCED SECURITY MEASURES ENFORCED AT RECOVERY SITES

One of the controls put in place for the purpose of this test included the blocking of traffic from each recovery site to the production network at the firewall level. This included access to VoIP phones, corporate email, network file and print services, production hosts, etc. Being the first annual test to strictly enforce these restrictions, recovery team members were forced to be creative in their troubleshooting methods, often crafting tools and processes on the fly, as might be the case in a true disaster scenario.

Another security control put in place includes the omission of command-line access for recovery team members. In its place, a TOOLBOX menu (command-line replacement app) has been implemented 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 test.

In hindsight, recovery team leaders had actually anticipated even more obstacles and issues than were observed, given the number controls added to this year's test. The ability of teams to quickly identify these obstacles, evaluate their options and navigate around them provided a valuable learning experience. A key takeaway from these increased restrictions underscore the value of designing these simulated recovery events to closely reflect actual disaster scenarios.

SAGE DIRECT DISASTER RECOVERY TEST

Although this key statement processing vendor has participated in past recovery tests, 2013 marked the first time both parties performed recovery tests simultaneously, each involved as a participant in the others' test. For the purpose of this test, we were able to generate and securely send encrypted statement files from our recovered host in NY to our redundant FTP server at our secondary (HA) datacenter, and then to the redundant host at SAGE Direct's offsite office location for processing. From there the completed files were sent 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. Details from the SAGE Direct recovery test are available in a separate report.

AUTOMATED CLEARING HOUSE TRANSMISSIONS

Multiple alternate options exist 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 our FRB "Buddy Bank" partnership with Honor Credit Union. Since this method had not been tested since 2011, it was included in the 2013 test. (As noted elsewhere in this report), we learned that the process required from the FRB to initiate "Buddy Bank" transmissions had changed since our last test. These changes have been noted in our documentation for future use in case this method for ACH transmissions is required.

ITSME247 APPLICATION TESTING

Also included in the annual recovery test is the availability and functionality of the ItsMe247 application hosted on the redundant stand-by server pool at the secondary (HA) datacenter retrieving data from the recovered host in NY. During this test, internal and remote users were able to point their browsers to the recovered site (without interruption to the production 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.

For future tests, we will look to expand the scope and objectives for the ItsMe247 testing process including a more direct presence and involvement from the ASP Programming Team.

SYNCHRONIZATION OF DATA RESTORED FOR TESTING

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. 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 recovery testing on at the IBM BCRS hot-site location, a portion of the encrypted tapes required are shipped in advance of the recovery team. The most current daily tapes travel with the recovery team to the restoration site. Recovery tests are planned in advance and are performed parallel to production core processing. This 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. In an actual disaster scenario, there would be no application and configuration changes until the host has been recovered. To better accommodate these recovery test that include participation with production clients at “proxy” credit union locations, the synchronization of data and application versions requires consideration of shipping, travel, and restoration timing.

This was evident during this year’s test where proxy credit union PCs running current production version software attempted to access data on the restored host from a prior backup (for the purpose of testing). This slight differentiation of versions provided application error messages that, although easily correctable in this situation, could in fact present a greater impact under certain recovery scenarios (i.e. beta software users). As noted elsewhere in this report, a project has been launched to reevaluate the process for archiving and restoring data to see where efficiencies can be implemented and recovery of synchronized data and application versions more effective. Recommended changes will be implemented and tested at the next host recovery opportunity.

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. iSeries Administrators were not able to configure PCs at the secondary (HA) datacenter for IBM remote access control of the recovered host due to insufficient privileges on the local PCs. This was resolved by escalating privileges for iSeries Administrators on each recovery site PCs.
2. As a result of the firewall "air-gapping", network administrators at the secondary (HA) datacenter were not initially able to access/manage the firewall appliance at the IBM recovery site, nor were they able to access/manage proxy client firewall appliances for configuration during proxy testing. A configuration change was required on the firewall at the IBM recovery site.
3. Early in the restoration process it was learned that a required tape was not included in those that traveled with the recovery team members to the IBM BCRS facility. Vital information on this tape included necessary data to enable the decryption of the remaining tapes. This forced recovery teams to brainstorm alternate methods of transmitting the data to the recovery site while honoring the assumptions established for this test (that the production datacenter is not available), short of sending another team member on the next plane to NY. Recovery teams were able to securely transmit the needed data from an alternate location (surviving site) to the recovery host in NY. In addition, lost recovery time was negated by making effective use of multiple tape drives for portions of the restoration process.
4. During the restoration process, the recovery of the "TOOLBOX" (command-line replacement app) required the use of command-line access. This required intervention by an iSeries Administrator. Modifications to the "TOOLBOX" application will be made and tested during the next system restoration opportunity.
5. It was discovered that some of the encrypted system password databases stored on the monthly DR/DVD were not current versions. Recovery teams were able to retrieve current system password database files from an alternate location at a surviving site. See "Future Recommendations" below.
6. Restoring the daily configuration file on the redundant 400ftp server did not create new directories. This was due to a permissions issue on the stand-by host. (Issue resolved for future tests).
7. Procedures for initiating and configuring FRB ACH "Buddy Bank" had changed since the last time this process was tested (2011). Documentation has been updated.

FUTURE RECOMMENDATIONS

1. A tape containing critical data required to decrypt all other tapes did not travel with the recovery team to the remote location. A review of the procedures followed before recovery teams leave for the remote site need to be reevaluated to ensure travel teams are properly prepared and equipped (media, equipment, plan documents and diagrams, etc.). These procedures should be documented in a manner that assumes a "hurried scenario" during an actual disaster (confirmation steps).
2. Server-side application data restored on the recovered host did match the client-side (production) application version resulting in some version error messages for proxy credit unions.
   a. The procedures for selecting and restoring data on the recovery host should be reviewed to ensure that recovery tests include data that is as current as feasible.
   b. CU*BASE/GOLD USER passwords that had been changed in the days since the media was shipped to the recovery site resulted in some proxy test participants and recovery team members needing to recall their previous passwords.
   c. System errors were generated during the EOD procedures regarding missing project libraries due to incorrect application versions restored on the recovery host.
3. System and application passwords that are critical during the first hours of a recovery need to be accessible to all critical business units company-wide, not just IT recovery team members. Although select password databases are archived, a project should be considered to archive all employee's password databases and to replicate those databases to surviving datacenters in the case of an actual disaster.
4. Reevaluate the procedures for archiving data stored on the monthly DR/DVD media to ensure data is current, and identify additional files and documentation that would be beneficial during an actual recovery event.
5. Future tests involving ItsMe247 should include an increase in participation from the ASP Programming Team as recovery scope and objectives are enhanced (especially due to personnel recent changes within the department).