CU*ANSWERS ITEM PROCESSING DISASTER RECOVERY TEST REVIEW

EVENT DATE: 12/12/2011

Revision Date: 1/6/2012

SUMMARY

As part of a robust business continuity program, CU*Answers actively tests recovery plans to ensure validation of processes and identify areas to improve recovery efforts and minimize impact to the organization and its major stakeholders.

This past year the Item Processing department migrated operations to a new application, Image Center. This dramatically changed the way Item Processing performs its daily operations and functions. A goal was set to test recovery of critical core operations at an alternate site by the end of 2011.

This particular event was especially noteworthy due to the fact that all previous recovery tests were performed under an annual contract with the application vendor (Jack Henry and Associates) at the vendor's site. JHA does not provide disaster recovery services for the Image Center platform. This test was performed using internal CU*Answers staff, relying on the vendor (Profit Stars) only for remote application support (if needed). Image Center test servers were recovered at the Muskegon datacenter.

Although we allowed ourselves 16 hours for the duration of the test, the recovery teams were able to successfully complete all steps within 8 hours. The test was performed in a sandboxed environment, parallel with production servers. Our clients experienced zero downtime or disruptions during this test. Considering that this was the first recovery test for this new application performed by our own staff on our own premises, the event was immensely successful, exceeding our expectations.

EVENT REVIEW

Data volumes for the Image Center application are stored on the SAN environment at the 44th street datacenter. Volumes are replicated to the SAN environment at the Muskegon datacenter. For the purpose of this test, two (database and application) of the four (database, application, two web servers) servers that comprise the applications were imaged and virtualized on our VMware server at Muskegon.

In preparation for this test, replication of data was interruptions on the morning of Friday (12/09). On the morning of Monday (12/12) we performed our test by retrieving data from (12/09) and processing it within the sandboxed environment (virtual servers). Firewall rules were set in place to ensure that the Image Center servers at Muskegon could not communicate over the network with production Image Center servers at 44th street. This allowed us to perform the test in parallel with production operations.

The Item Processing business critical functions performed during this test included:

- Downloading test files from FedLine
- Importing files to servers at Muskegon
- Performing reject/repair procedures
- Client Totals Reporting/Comparisons
- Building and Transmitting distribution files [online and offline (CUNW) clients]
- Creating manual return files
- Uploading test files to FedLine
- Outgoing Exception Report creation and printing

The test process began on Monday (12/12) at 9:00 AM and completed by 4:45 PM. Participants operated from the 44th street offices, connecting to the workstations and servers at the Muskegon datacenter using Microsoft Remote Desktop clients.

CHALLENGES

Many of the documented challenges below are the result of our efforts to perform a recovery test parallel with the production environment (no downtime for clients). In an actual disaster recovery effort (recovering the production environment), most these challenges would not exist.

1. The replication of data between 44th street and Muskegon SANs was intentionally interrupted at 9:00 AM Friday (12/9) for the purpose of this test. Replication was re-initiated following the completion of the test at 5:00 PM on Monday (12/12). During the weekend, the virtual servers lost connectivity to the SAN volumes in Muskegon. When connectivity was restored, the drive mappings (CONFIDENTIAL) were not consistent with production. This generated errors early in the test process. The problem was identified and corrected immediately. The processes of confirming drive mappings will be documented for future test preparation.
2. The two production servers that were used for the purpose of the test where virtualized back in mid-Summer. It was assumed that the dynamic volumes (data) were part of the SAN replication process. We learned that a folder (CONFIDENTIAL) on the application server is used to store temporary check images during processing. The actual check image is stored on a replicated volume. This temp image is used only to display the image in a browser. For the purpose of this test, we copied the contents of the production server to the recovery server. If this were an actual disaster, we would have restored the folder from backup NAS or tape. A project has been imitated to move this folder to a replicated volume.
3. Access for workstations at Muskegon to FedLine site was blocked by the firewall. This was an expected event. A firewall change was made to allow access during the testing process. This step will be added to the documentation for future tests. Regarding FedLine site, it was noted that during the test, both live data files and data files used in the test could be seen on the site (expected). Careful attention was made by operations staff not to process the files used in the test on the production servers. This would not occur during a true disaster or if future tests were performed off hours.
4. Using the Microsoft remote desktop clients posed one issue when local drive mappings overwrote the remote desktop drive mappings creating a potential scenario where files used for testing could be uploaded to the production server. Disabling local drive mappings corrected this issue. This would not pose an issue if the test was being performed at the Muskegon datacenter. Steps to disable local drive mappings will be documented for future tests.

5. The (CONFIDENTIAL) FTP client on the Muskegon workstation was configured to upload files to the IP address of the production Image Center server at the 44th street datacenter. This was corrected to point to FQDN (server name). Documentation for future tests will provide steps to check and correct this. For the purposes of this test, we modified the workstation's hosts file entries.
6. Test file submitted to the server in Muskegon was stuck in "pending" status. It was determined that the service that processed such files was not running. The service was started on the server and file was processed. This problem was the result of the drive mappings on the SAN not matching that of production (as noted in no. 1). Documentation for future tests will provide steps to check and correct this.
7. Attempt to submit ACH file to (CONFIDENTIAL) from Muskegon server was unsuccessful. Determined that Pentasafe application on (CONFIDENTIAL) was blocking the transfer (coming from an alternate IP address). This was corrected and has been added to recovery documentation.

CONTINUING EFFORTS AND RECOMMENDATIONS

1. Determine annual schedule for future tests.
2. Identify functions and processes (core but not necessarily "critical") to include in future tests to expand the scope.
3. Perform future tests with staff at the Muskegon datacenter.
4. Network Services is initiated a project to relocate the backup FedLine appliance from the 28th street datacenter to the Muskegon datacenter by the end of fiscal year 2012.
5. Virtualize current physical production servers and move them to the VM cluster at 44th street. This would allow more current "snapshots" replicated to the Muskegon VM server. Note that for this test (see Challenges no. 2) the two servers were virtualized using snapshots from mid-Summer. The process to perform these physical-to-virtual snapshots is manual and problematic. By moving the production servers to a VM server, this process could be automated and less problematic.
    a. A project proposal is being created to help determine the feasibility of this recommendation.
6. Network Services is investigating the feasibility of implementing changes to the SAN that would allow production replication to continue to Muskegon during future disaster recovery events in Muskegon.
7. Network Services has initiated a project to move the (confidential) folder in Challenge #2 to the SAN by the end of January, 2011.