OVERVIEW

The annual CU*Answers Disaster Recovery Test was conducted on 5/05-5/07, 2015 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 2015 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.

For the purpose of this test, 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. For example, the procedures for restoring the IBM host operating system on the morning of May 5 were performed by the newest member of the iSeries Administration team and first-time recovery test participant.

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/mobile 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:

- **Clarkston Community Credit Union**
  - *(Proxy credit union)*
- **Notre Dame Federal Credit Union**
  - *(Proxy credit union)*
- **Kellogg Community Federal Credit Union**
  - *(Proxy credit union)*
- **FedLine**
  - *(ACH transaction)*
- **SAGE Direct**
  - *(Member notification file creation and transmission)*

SAGE DIRECT MEMBER NOTIFICATION TRANSMISSION TEST

For the purpose of the 2015 test, recovery teams were able to generate and securely transmit encrypted notification files from our recovered host in Sterling Forest to the redundant GoAnywhere server at our secondary (HA) datacenter, and then on to the host at SAGE Direct's disaster recovery location for processing. From there, the NOTICES files were transmitted securely to SAGE Direct's alternate print provider (Presort Services) for printing and mailing (total of 214 member notices were included in the test). These files were generated, transmitted, processed, printed and prepared for mailing without the use of either CU*Answers or SAGE Direct's primary production facilities.

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 through the redundant FedLine VPN connection at the secondary (HA) datacenter. This redundant VPN option is tested multiple times each year during our HA "rollover" exercises with live data. An alternate option is the use of the FRB "Buddy Bank" partnership with Honor Credit Union. For the purpose of the 2015 test, recovery teams prepared, transmitted and received "test" files on the restored host using the redundant FedLine VPN at the secondary datacenter.

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 2015 test, internal and remote users were able to point their browsers to the recovered site, authenticate, and check application features. At this time, servers hosting OBC (Online Banking Community) are not installed at the secondary datacenter and were not included in the application testing.

CLIENT "PROXY" CREDIT UNION TESTING

Perhaps the most significant factor that determines the success or failure of the disaster recovery test is whether or not in-network client credit unions can access the restored host at the hot-site and perform daily CU*BASE/GOLD functions. Since the recovery test is performed parallel to the production environment (without downtime), the process to coordinate off-hours credit union connectivity to the hot-site is carefully planned and executed. For the purpose of this test, three "proxy" credit unions were selected on behalf of all in-network credit unions. One-by-one, these proxy credit union networks were redirected to the host site and CU*BASE/GOLD connectivity with session encryption confirmed. Test procedures at the credit union included multiple user access and data integrity checks by comparing report balances.

THIRD-PARTY EFT VENDOR TESTING

In addition to selecting a small number of "proxy" credit unions to participate on behalf of all in-network credit union clients, previous recovery tests included a sample of third-party EFT vendors to test connectivity with the recovered host. This third-party testing was performed by installing temporary network appliances provided by each vendor at our secondary datacenter and certifying communications back-hauled through to the hot-site. These tests were performed parallel to the production environment, required several months of planning and preparation, and added significant costs to the testing process.

Beginning in 2014, CU*Answers initiated projects with third-party EFT vendors to install permanent network communications at the secondary datacenter, adding redundancy to the production environment and significantly reducing recovery times. Several vendor projects have been completed with more scheduled throughout 2015. Since the redundant third-party network components are added to the production environment, testing connectivity to the recovered host at the hot-site in an offline environment could present the risk of interrupting production traffic. For this purpose, testing third-party EFT vendor communications at the secondary datacenter will now be performed outside of the disaster recovery test, either stand-alone or as part of the scheduled High-Availability (HA) Rollover events.

THE SHIFTING ROLE OF DISASTER RECOVERY

Maintaining a tertiary hot-site location that is compatible with the current production operational environment and also complies with shrinking recovery time and point objectives is getting more difficult with each day. As the network continues to expand in scope and complexity and the demands on system and application availability increases, the strategic focus shifts from that of recovery to high availability.

Moving forward, there will be more investment and attention given to utilizing redundant networks and components during rollover events in a live environment where core processing is provided from the secondary datacenter. This will include connectivity to hosts and applications from third-party vendors and technology service providers. This strategy is designed to best prepare the network for future large-scale disruptions at the primary datacenter. Disaster recovery strategies will focus more on the ability to quickly and effectively restore the core processing host from “scratch” using the data available on tape media stored off-site. The location and source of the recovery site may change over time.

This shift in focus is aligned with a project expected to be initiated in 2016 that relocates the high-availability site, effectively increasing the distance between primary and secondary datacenters and provides operational support in the event that local staff are not available in a large, regional recovery effort. More about the 2016 relocation project will become available as plans and dates are finalized and approved.

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. During the initial stages of the recovery effort, it was determined that the recovery host authentication credentials and tape device naming convention provided by IBM did not match those requested during pre-event planning session.

    a. Working with IBM support personnel, iSeries Administrators were able to reconfigure these credentials and device configuration enabling them to proceed with the restoration.

2. Enabling the LAN interface port on the hot-site firewall was not successful. The interface port was determined to be non-functioning (possibly a hardware failure).

    a. Local recovery team members were able to relocate the patch cable to an available port while remote firewall administrators configured the appropriate access rules for the LAN interface on the new port.

    b. This is the same firewall appliance that experienced issues during the 2014 disaster recovery test. In between the 2014 and 2015 tests, the firewall was returned and an updated firmware applied. Due to recurring issues, a new firewall appliance has been budgeted to replace the existing unit.

3. During the system restoration process, iSeries Administrators experienced licensing errors when launching the Client Access application.

    a. This is similar to the error received during the 2014 recovery test. During the restoration process, some procedures (while automated in production) were disabled to prevent any potential interruptions to production core-processing (i.e. notifications, etc.). These procedures were performed manually for the purpose of the test. This created some instances where certain modules (in this case, Client Access) required reinstallation if not installed in the sequence expected by the system. Reinstallation corrected the licensing error.

    b. This is an example of having to alter procedures for the purpose of the test (performed parallel to production) where in an actual recovery effort, these procedure modifications would not be required.

4. It was determined that multiple versions of the same file (CUBASEFILE) exists on separate tapes used in restoring the CU*BASE environment. This resulted in outdated login credentials overwriting current credentials for users who had recently changed their system passwords.

    a. The most current version was restored and logins confirmed. Recovery procedure documentation has been updated to select the most recent version of the system file.

5. The restored host detected a missing file (RBTSYSLIB) in the OPERATOR library list.

    a. The library restore process was performed again and the affected system file deselected/selected to correct the issue.

6. The EOD/BOD process detected a missing EOM file for a recently converted credit union.

    a. Due to the timing of the recovery test (relative to the first of the month), a recently converted credit union's EOM library file was not included in the tapes shipped to the hot-site location. In an actual recovery effort, the most recent set of tapes will be used to restore the host.

7. When attempting to generate the NOTICES file, the host detected a missing ARCSAGE table.

    a. Due to the nature of this data (no history kept), this table is not archived to tape. In a recovery effort, this table is to be created. Procedures to recreate the table have been added to the recovery documentation.

8. Initial proxy credit union users experienced a (Seagull) license error when first launching CU*BASE/GOLD from the restored host.

    a. It was determined that the procedures for activating the Seagull license on the restored host were not fully completed. Documentation has been updated to test license activation prior to performing proxy tests in future recovery efforts.

9. During one of the proxy credit union tests, a remote credit union user had unintentionally logged on to the restored host during the proxy test window.

    a. Recovery teams monitor this type of access during the proxy tests to ensure that only users participating in the test are accessing the data on the restored host. Future proxy test communications will include language that emphasizes the need to ensure that only authorized test users access the host during the test window.

10. During one of the proxy credit union tests, it was learned that an automated process configured at the credit union had attempted to pull data from the restored host during the proxy test window.

    a. This is another example of the growing complexity of the network and our ability to safely perform disaster recovery tests parallel to the production environment. Future proxy test communications will include language that emphasizes the need to ensure that no automated tasks are performed during the test window.

FUTURE RECOMMENDATIONS

As mentioned in previous reports, the amount of planning and resources required for the annual disaster recovery test just to make sure that there are no interruptions to the production environment has exceeded that required to perform the test itself. We have now crossed the line 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 perhaps never more evident than during the 2014 recovery test that happened to fall during a week where an emergency HA rollover was required.

While the overall scope of the current recovery test has decreased compared to previous recovery tests, significant knowledge and awareness is 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.). *See section above "The Shifting Role of Disaster Recovery".

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