DEPARTMENT OF TECHNOLOGY AND INFORMATION
STATE OF DELAWARE
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

The Honorable James L. Collins, Chief Information Officer

NASCIO STATE RECOGNITION AWARDS 2015

DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION'S COMBINED DISASTER RECOVERY AND CONTINUITY OF OPERATIONS PROGRAM

CATEGORY

Disaster Recovery/Security and Business Continuity Readiness

Project Start and Completion – October 30th – October 31st, 2014

Contact: Mike Hojnicki, Chief of Policy and Communications

Delaware Department of Technology and Information

Michael.Hojnicki@state.de.us 302-739-9654

Delaware's Combined COOP and DR Exercise - Executive Summary

The Delaware Department of Technology and Information (DTI) is the central IT support agency for all of state government. DTI provides enterprise-wide data management, storage and telecommunications for all three branches of state government. Additionally DTI provides email services for all of Education K-12, which includes 19 separate districts and 20 Charter schools. The Delaware Continuity of Operations Program (COOP) crosses multiple boundaries and forged partnerships between government agencies that support critical services for citizens and the state's enterprise IT organization. The Department of Technology and Information (DTI) has developed a six-phase strategy:

1. Education and Senior Leadership Approval
2. Business Impact Analysis
3. Plan Building
4. Emergency/Notification/Crisis Communication
5. Testing the Plan – COOP Drill
6. Maintenance

A prioritized three tier model was developed with the Delaware Emergency Management Agency. Tier I organizations are necessary for immediate public safety and public health response or those essential to the preservation of continuity of government. This includes the Governor's office. Tier II agencies are those necessary for follow up support to emergency response and recovery efforts or provide non-emergent support to response and recovery efforts. Tier III includes all other state organizations.

In October 2014, as part of our Disaster Recovery and Continuity Operations Program, we simulated a major outage to State critical IT systems. Our scenario included a monster F3 tornado that pummeled a 2-mile stretch in central Delaware. The complex housing DTI's main office and data center was especially hard hit, resulting in a complete loss of the data center.

DTI's Emergency Response Plan was activated, and our teams responded to our out of state hot site provider, SunGard Availability Services. Simultaneously, DTI teams reported to our in the state alternate work location. The DTI Team at the out-of-state site successfully restored DTI-managed criticality 1 and 2 systems within 12 - 48 hours, focusing first on health and public safety systems. The DR exercise staff participants worked around the clock, maintaining two 12 hour shifts.

In tandem, we followed our COOP Plan to restore Critical Business Services at our alternate work location. A phone and data network was established within 30 minutes and Service Desk operations resumed after a seamless enterprise-wide transfer. This was accomplished while maintaining normal service desk operations that include answering about 300 service request calls per day.

Just like a fire drill, a simulation of a major IT outage improves our ability to respond and recover from an actual event. Here in Delaware, we have made great progress in protecting our critical information infrastructure. Lessons learned were gathered from participants in all parts of the exercise and an After Action Report was published.

Description of Business Problem and Solution

Our nation has experienced a variety of natural disasters/weather related incidents in the past year. Bitter cold, abnormally high snow accumulations and tornados have threatened and impacted lives and economies in many states and including Delaware. DTI's Disaster Recovery and Continuity of Operations Teams (DR/COOP) are dedicated to continuous testing and preparations in the event that Delaware state government faces a catastrophic enterprise-wide disaster. A unique combined DR/COOP exercise took place on Thursday, October 30 and Friday, October 31, 2014 in two remote locations under just this scenario.

Delaware is unique in several ways due to our small size, geographic location and completely centralized IT enterprise network, data storage and critical infrastructure. Within our 90 mile length we have the urban corporate capital of America, Wilmington, rich farm resources in the center of the state, and the Atlantic Ocean coastline in the southeast. We're home to Dover Air Force base a major supply/support base and within one to four hours' drive time of New York City, Philadelphia, Baltimore and Washington D.C.

While spared the brunt of Hurricane Sandy that devastated much of New Jersey and New York's Atlantic coastline, Delaware is within a hurricane threat area, and experiences dangerous Nor'easter storms several times each year. We're subject to terror and cyber threats due to the presence of the Air Base and location within northeastern America's megalopolis.

The Department of Technology and Information is responsible for enterprise-wide telecommunications and management of all centralized applications and infrastructure. This includes all three branches of government and 19 separate K-12 school districts and 27 charter schools. Governor Markell's Executive Order 20 – More Effectively Utilizing Information Technology Resources to Drive Cost Savings in State Government - calls for the optimization of IT operations and staffing statewide. DTI physically houses the major data center for all of state government.

The purpose of the Department of Technology and Information's (DTI) Enterprise Disaster Recovery Test was to simulate an IT infrastructure outage due to an F3 tornado that leveled Delaware government's data center which supports the entire State. The outage affected the enterprise Public Safety, Financial, Pension, and Payroll/ Human Resource Systems, GIS, and Mainframes. The following support systems were also scheduled for recovery in support of this exercise: Disaster Recovery Master Server, Terminal Server for remote access, Virtual Server Environment, Enterprise Tape Backup System, Extensible Markup Language Firewall Environment (XML), and Secure File Transfer Protocol server.

The Enterprise Disaster Recovery Test occurred at our Hot Site provider SunGard Availability Services, located outside of Delaware over two consecutive days. The test was performed by employees of DTI: Data Center & Operations Team, Systems Administration Team, Systems Engineering Client Server Team, the Telecommunications Team, and the Business Continuity and Disaster Recovery Team.

Twenty-six DTI staff members were deployed to SunGard. The test also included personnel from the following participating agencies:

- Government Support Services – ERP - Payroll and Human Resource systems
- Division of Accounting – ERP – First State Financial accounting system
- Pension Office – Pension payroll & benefit systems
- Judicial Information Center – Public Safety/Law Enforcement
- Department of Labor – Unemployment Insurance Benefits
- DELJIS – Law Enforcement/Judicial systems
- Division of Revenue – Tax & Business registration Systems

DTI would not have been able to accomplish the validation of the restores without the help of the state organizations listed above. Over 30 people in these agencies tested systems for full functionality while still maintaining day-to-day operations.

DTI continued the use of the DR Master Server and Terminal Server to control network communications for customers who needed access to the recovered environment during the test. A dedicated test environment was established so that system communications are restricted to the isolated DR environment and therefore not conflict with production systems. The dedicated DR environment enables production to stay running during the simulated outage. Due to the ever changing technical environment, procedures and documentation are updated in a continuous process to keep recovery documentation current.

To make certain that the data recovery was not just functional but complete, a data restore date, prior to the exercise was selected and all data restored to the recovered systems during this exercise was required to reflect the respective date stamp in order to verify that the recovery of system data was successful.

On Thursday, October 30th, the hot site team began restoring DTI managed criticality 1 and 2 systems within 12 - 48 hours, focusing first on health and public safety systems. DTI had enough personnel on site to have two 12 hour shifts to ensure recovery continued through the test duration. DTI's Senior Staff instructed the DTI Business Continuity/Disaster Recovery Team (BC/DR) to activate the alternate location in state and deploy resources to stand up the network. Essential employees were also notified of the incident and put on standby.

At 6:30am on Friday, October 31st, the Chief Operations Officer leveraged DTI's enterprise emergency notification system to instruct essential DTI employees to immediately report to the alternate location. Exercise participants understood that none of the resources formerly available in DTI's main headquarters were available to them. The staff were to immediately begin their appointed COOP responsibilities to support continued state government business operations.

Once onsite at the alternate location, Senior Staff established a Command Center to discuss the events affecting normal operations and establish appropriate communications for release to staff and media. Conference calls were conducted regularly between Sr. Staff, customer client agencies and the disaster recovery site. All health, public safety, and financial mission critical applications were restored and available for agency use within 12 – 48hrs.

Significance of the Project

Delaware government's IT community is well aware of the very real threats that exist to disrupt the enterprise IT system and disrupt continuity of operations, not just for government itself, but for our citizens. If core government services were unavailable for an extended length of time the effects would immediately impact Delaware's businesses, economy and citizens directly. Delaware is host to thousands of corporations and its economy is diverse, from agriculture to manufacturing to tourism. Public Health and Safety First Responders depend on enterprise systems for evacuation routes, deploying physical and people resources and making needed materials purchases. Delaware's geographic location makes it particularly vulnerable to catastrophic weather events and cyber/terror threats.

Even with this knowledge it can be difficult to secure executive support for a comprehensive DR/COOP test simply because of the budgetary costs and people resources. Many of the state's IT personnel are responsible for multiple projects and programs and taking them away from their primary business for even a day or two can be problematic. Executive Support and DTI's commitment to customer service and strong client relationships was key to winning the support of top level agency managers for the critical testing and validation procedures.

Although there were several difficulties with restoring the mission critical applications at the hot site, the team worked together to successfully overcome the challenges faced during the exercise. The test included an added simulation of primary System Administrator support personnel being unable to work for the disaster recovery test. However alternate System Administrator support personnel from within DTI were able to recover the systems in record time. The team continues to learn valuable information on the recoveries of critical state government systems.

This DR portion of the test was accomplished with coordinated teamwork from the following DTI teams:

- Data Center & Operation
- Systems Administration Team
- Client Server Engineering Team
- Telecommunication
- Desktop Support
- Business Continuity/Disaster Recovery Team
- Agency Testing/Validation Teams

The COOP portion of the test was accomplished with coordinated teamwork from the following additional DTI teams:

- Enterprise Desktop LAN
- Enterprise Service Desk
- Mainframe Services
- Customer Engagement Team
- Applications Delivery
- Telecommunications
- DTI's Senior Management Team
- Business Continuity/Disaster Recovery Team

These combined teams included approximately 25% of DTI's total staff during a normal work day.

Benefit of the Project

DTI conducted an extensive and comprehensive exercise that included both restoration of systems at our out-of-state hot site, and continuity of operations at our primary alternate location in state. The Telecommunications Team recovered the network and service desk phones within 30 minutes of arriving onsite. All public health, public safety, financials and mission critical systems were restored within 12-48 hours and available at the onset of the COOP portion of the exercise. All DTI and customer testing requirements were successfully achieved during this exercise. The DTI Incident Command team responded quickly and established a schedule to ensure routine updates and stay abreast of event activities. Considering the scope of this exercise, and the success with which all the stated exercise objectives were achieved, the event was a tremendous success.

Few, if any, states have complete responsibility for providing enterprise systems and networking for all three branches of government as Delaware does. Add to this the entire education K-12 community with 19 separate districts and 27 charter schools, and it is clear that DTI faces huge challenges. The ramifications of a natural or man-made disaster are well understood and Delaware's public safety, public health and economy depend on robust 24/7 operations regardless. This combined DR/COOP exercise proved that DTI staff have the technical skills and dedication required to face the most difficult of challenges.