the Availability Digest

www.availabilitydigest.com
@availabilitydig

Iowa's Data Center Taken Down by Fire

April 2014

In the article Fire in Your Data Center: No Power, No Access, Now What?, published in Government Technology,[1] Robert Von Wolffradt, the CIO for the U.S. State of Iowa, described a fire that took down the Iowa's primary data center for the entire state. He relates an orderly progression to restore service and concludes with several lessons learned. The fact that he took the time to publish this account is a service to all who are responsible for their data centers' uptime.

The Fire

On Tuesday, February 18, 2014, the Iowa legislature was in session. Payroll processing for state employees was scheduled for that evening. Weather forecasts called for severe blizzards within the next two days, and plans were being prepared for coverage to ensure that technical IT resources would be available during the blizzard.

Shortly after 3 PM, the building lost power and evacuation was commanded. The staff had been through such drills before and considered this to be just another one. However, as staff assembled in their designated areas, reports of fire and smoke began to be received. An attendance of evacuees was taken, and the preliminary reports were confirmed. The staff evacuated the building without incident. The fire department and police blocked reentrance to the building by any of the staff.

The first step was communications. Within thirty minutes of confirming the reports of fire, the CIO briefed the governor's chief of staff, director of management, and the governor's spokesperson. Since the legislature was in session, reporters were already present; and they too were briefed.

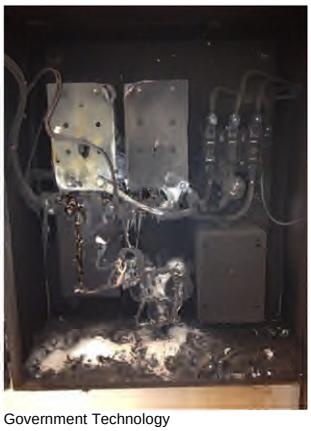
The next step was to assess the seriousness of the situation and the steps to be taken to recover IT services. The technology response team had evacuated to a nearby building and began to plan the command-and-control response. Meanwhile, the police and fire department were being encouraged to allow access back into the data center, but this took a while until they were satisfied that there was no longer any danger.

The Recovery

Conference call schedules were set up with the various teams within the IT staff, and the first round of updates was completed by 4:45 PM. The teams were broken up into work streams and had completed a preliminary sequence of restoration processes by 5 PM.

[1] Fire in Your Data Center: No Power, No Access, Now What?, *Government Technology*; March 20, 2014.

Cleanup


Government Technology

Shortly after 5 PM, the top echelon of the general services staff was escorted into the building by the fire department. The smell from the FM-200 fire suppression discharge was especially pungent. The source of the fire was quickly identified. It was a wall-mounted electrical suppression unit which prevented power surges from entering the data center.

The first issue was to restore power, bypassing the failure point, and venting the data center so that it was habitable. This was complicated by the fact that the air conditioning chillers were on the same power source and had to cool the data center before the servers could be rebooted. The general services staff bypassed the failed electrical suppression unit and restored power. They adjusted controls to allow for exhaust and venting.

The damage to the data center was reviewed, and cleanup efforts and fire watch controls began. One problem was that physical access controls had to be disabled because the data center doors had to be opened for venting. It was necessary to position staff at the doors to control physical access.

Fortunately, none of the IT equipment was damaged.

The Failover Decision

The State of Iowa maintains a backup data center, and a decision had to be made whether to failover to the backup systems or to try to restore the primary systems. This is always a difficult decision because of the chance that the backup systems will not come up, typically due to configuration drift.

One factor in the failover decision was the need to avoid idling staff for a prolonged period of time. On the other hand, staying with the primary data center risked potential impact on the UPS (Uninterruptible Power Supply) and the servers, disks, and network equipment that were now exposed to raw utility power without the protection of the electrical suppression unit.

Based on cost, time, and risk, it was decided to attempt to restore the primary data center. Failover testing had shown trials and tribulations when failing over to the backup data center and the subsequent time and workload associated with falling back to the primary center once it was back in operation. Although the staff had good experiences failing over to the backup, it was felt that time and money could be saved by giving the primary data center a shot first.

However, just in case, by 6 PM the backup data center was staffed and ready to go. By this time, power had also been restored to the primary data center.

Service Restoration

Meanwhile, the pressure to restore services was increasing. Management needed to know if it was safe for the almost 1,000 evacuated staff members to reenter the building and whether they would be able to use IT services the next day. Even more pressing was that payroll processing hadn't started, and direct deposits had to be made to employee bank accounts the next day.

The Department of Transportation needed its cameras with the impending blizzard conditions. The Department of Revenue needed to process tax collections. The Justice Department needed to process claims and fee payments. Accounting needed to process USD $162 million in payments, including direct deposits. State websites were unavailable to the state's residents and businesses.

The building and data center was deemed to be safe at 6:30 PM. The IT response teams returned to the data center and began the service restoration process. The staff leveraged the Iowa Homeland Security

alert notification system to send status updates to agency directors. State leadership continued to be informed throughout the event.

The restoration of services within the data center depended upon interdependencies between application and on the priority of services:

- 9 PM Feb. 18 – The data center was cleaned of residue. SANs (storage area networks), firewalls, and the core of the network were restored.
- 11 PM Feb. 18 – The service desk, DOT cameras, virtual machines, and financial systems were restored and put into operation.
- 2 AM Feb. 19 – Several other systems were restored, including SQL, mainframe, email, tape library, some justice systems, additional firewalls, DNS, Web email, authorization and authentication, major websites, and agency systems.
- 3 AM Feb. 19 – Print services, federal systems interfaces, additional justice systems, and agency applications were restored.
- 7 AM Feb. 19 – All outage and service calls were routed through normal systems and processes.

Total recovery from the fire was accomplished in sixteen hours, with critical services being restored within eight hours. At this time, the recharge of the fire suppression system was scheduled as was the replacement of the failed electrical suppression unit. Logs and team minutes were collected for analysis, and staff were returned to their normal duties.

Lessons Learned

The staff focused on reviewing the entire restoration process and came up with a list of lessons. In the CIO's words, the lessons included:

1. Test complete loss of systems at least once a year. No simulation - take them offline.
2. Consider diversifying major enterprise system facilities from each other (email in separate facility from payroll, or others, etc.).
3. Coordinate closely with your facilities and human resources functions. They are our best friends in events like this.
4. Schedule a complete review of your data center's electrical systems and ensure they are fully documented.
5. Allocate personnel to recovery actions as soon as possible and then release folks for follow on shifts.
6. Over-communicate.
7. Assume the worst, plan accordingly, and thank your dedicated employees.

Summary

An important effort that is often overlooked is communication. There is a wide range of communication that is required in an incident such as this. Of course, management must be kept informed. Breaking the IT staff into teams with assigned duties required tight communication between the teams. The affected agencies and other users must be kept informed of progress and the expected recovery time of services. The press should be kept informed so that the public understands what is happening. Local officials with a need to know, such as fire, police, and government officials, must be kept abreast of the cause of the

incident and the progress being made towards its resolution. In all of these cases, the Iowa data center excelled at keeping people informed.

A difficult decision that had to be made by IT management was whether to failover to the backup data center or to try to restore the primary data center. Both have their attendant risks and costs. In this case, it was decided to restore the primary data center. If the alternate decision had been made, would the failover have been successful? Only periodic testing can answer this question. Make sure that you can fail over to an operating backup center, and don't rely on just faith and hope. Failover faults are one of the major causes of system outages. As the CIO said, "Test complete loss of systems at least once a year. No simulation - take them offline." True, failover tests such as this carry a level of cost and risk. But the cost and risk of a failover fault can be much worse.

Finally, publishing the procedures, successes, failures, and lessons learned in an incident such as this, as was done by the State of Iowa CIO, is a benefit to us all. We wish more organizations would adopt this practice.