Preparing Your Fund for the Unexpected

Abstract: This paper discusses the unique contingency planning needs of multi-employer trust funds, with an emphasis on data protection and restoration.

Introduction

Natural and man-made disasters can occur with little warning, leaving organizations without a contingency plan scrambling to maintain operations. As benefit administrators, multi-employer fund offices provide critical services to members and their dependants, yet a 2006 survey by the International Foundation found that only 35 percent of funds had a disaster contingency plan (1)[i]. A surprising fact, since organizations without plans often face extensive service disruptions after a disaster; some never recover. According to Gail McGovern, President and CEO of the American Red Cross, "Studies show that between15 percent to 40 percent of businesses fail following a natural or manmade disaster" (American Red Cross). The reasons why organizations lack contingency plans are as varied as the arguments the Red Cross and others give in support of them. While it may be an unpleasant task, developing a plan can help limit the impact of unexpected events on the fund's operation and help ensure that participants receive the support and service they need.

Making a Plan

Contingency plans, or disaster recovery plans as they are often called, should be carefully designed to accommodate the unique needs of the fund and the fund office staff, routinely updated to reflect changes in the organization, and periodically tested and revised as needed. At a minimum, plans should identify possible threats to the fund's day-to-day operations and establish solutions for mitigating these risks. According to Disasterrecovery.org, an independent contingency planning resource, "The essential procedures to restore normalcy and business continuity must be listed out," and should include "the plan's steps for recovering lost data..." (3). Disasterrecovery.org argues that "plan steps that are well-constructed and implemented will enable organizations to minimize the effects of the disaster and resume mission-critical functions quickly." As part of the plan, the fund should also assign an individual or team responsible for recovering operations after a disruption in service and establish a process for communicating pertinent information to employees, members, trustees, vendors and others.

Protecting the Fund's Data

While the procedures and contact information in a written contingency plan can provide guidance during stressful situations, preventative actions, such as protecting the Fund's data with regular backups and selecting an alternate operations site, are key to the plan's success. The International Foundation found that 82 percent of organizations with disaster plans included business continuation provisions for "off-site storage of backup electronic and paper records" (3)[ii]. There are many data redundancy options available, including online downloads and backup

tapes. However, keep in mind that all electronic files should be encrypted to protect members' personal information and ensure compliance with HITECH. Files should also be verified for completeness and restorability. Ideally, backup tapes should be tested off site since machines with ill-aligned tape heads can produce and read their own tapes, but may have trouble creating viable tapes for use in other machines.

Once the fund has established a procedure for maintaining and retrieving backup data, consider choosing a contingency partner, such as a nearby sister local, who can provide office space during an emergency. Having a location where the data can be restored shortens downtime in the event the fund's location is inaccessible or non-operational. Nearly three-quarters of the groups surveyed by the International Foundation with a disaster plan had established an alternative worksite.[iii]

It Happened to Them: ISSI Clients Weather the Storm

Several ISSI clients have been impacted by hurricanes over the years. Thankfully, all the funds were able to resume operations following the storms, though some experienced prolonged service delays because they did not have a formal disaster contingency plan.

For example, prior to one storm, an ISSI employee had the foresight to remotely download data to our New Jersey-based server from a fund office in the hurricane's path; however, without an emergency contact plan, ISSI had no way to let the staff know that their data was available. ISSI worked with the fund's lawyer and a sister local in a nearby town to establish an alternative operating site before anyone in the fund office was even aware that their data had been saved. Had the fund established a contingency plan with contact information, and shared the plan with ISSI, they would have been operational within a day of the storm.

Having a formalized plan can also help fund staff follow the best course of action in times of crisis. Because the fund's operations are critical, and its data governed by legislative mandates, staff may need to follow emergency procedures that differ from the general advice provided by local news sources. For example, hoping to prevent power surge damage during a hurricane, one ISSI client followed a broadcast's advice and shut down all equipment. In the midst of the storm preparation confusion, the staff accidently left the backup tapes for the ISSI system in the fund office when they evacuated. Had the equipment been on, ISSI would have been able to pull data from the fund's server remotely. Alternatively, if the backup had been taken off site, the system could have been restored to another server. Instead, the fund was left without backup data and was down for an extended time while water receded from the floors below the office.

Small Problem, Big Consequences

Though the examples in this paper have focused on large-scale disasters, fund-specific crises, such as hardware failures, occur with more frequency and can cause long disruptions in service. Having redundant servers, either at the fund's location or offsite, can ensure the fund remains

operational in the event of a hardware failure. Just this month, an ISSI client was able to continue serving members despite a complete server failure. The fund maintained operations on an ISSI contingency server, established prior to the crisis. Without this planning, the fund office would have been down until the faulty hardware was replaced.

Even minor disruptions, such as power outages or connectively issues, can cause huge headaches for the fund. Though these events are typically short in duration, they still impact the fund's ability to serve members and should, therefore, be included in the fund's plan and preventative measures.

Conclusion

When preparing for the unexpected, it is important to choose partners who understand the unique challenges facing multi-employer funds. ISSI offers disaster contingency solutions that ensure a current replica of the fund's ISSI Benefit Administration System is always accessible and restorable from a secure, off-site location in the event that the fund office or ISSI server ever became unusable.

For more information on how ISSI can assist your fund with disaster contingency planning, please contact Kristen Lucas at (856) 910-9190 ext. 327 or KLucas@ISSIsystems.com.

---

[i] The International Foundation surveyed multiemployer trust funds, corporations, public employers, and professional service organizations. While 52% of total respondents had disaster plans, only 35% of funds had established plans at the time of the survey.

[ii] Percentages based on total survey results.

[iii] Percentages based on total survey results.

Works Cited

American Red Cross. "American Red Cross Launches National Ready Rating™ Program to Prepare Businesses, Organizations and Schools for Emergencies." *American Red Cross.* American Red Cross, 12 May 2011. Web. 14 June 2011.

Disasterrecovery.org. "Business Continuity/DR Step." *Disasterreovery.org.* N.p., n.d. Web. 14 June 2011.

International Foundation of Employee Benefit Plans, Inc. *Disaster Planning*. Brookfield: IFEBP, 2006. Print.