insight**On:**

Disaster Recovery – Is Your Contact Center Prepared?

With networks airing dramatic and disturbing scenes of inundated Gulf Coast cities and with the frightening magnitude of the tsunami in Southeast Asia still fresh in our memories, companies are more aware than ever that planning and preparation, particularly with regard to critical business systems such as the contact center, is of the utmost importance.

Both global events and legislative initiatives, such as the United States Sarbanes-Oxley regulations and the International Basel II framework, now demand that companies take a closer look at how they would support their contact centers in the event of a disaster. There are a number of factors your organization should take into consideration when building a comprehensive disaster recovery plan.

Companies are more aware than ever that planning and preparation, particularly with regard to critical business systems such as the contact center, is of the utmost importance.

Consider All the Possibilities

First acknowledge that the term "disaster" encompasses a lot of unpleasant possibilities. Get specific about the types of problems your contact center might face:

- **Facility disaster**
  The building is damaged.

- **Facility downtime**
  Power is cut from the facility or resources cannot get to the facility (usually weather related).

- **Component disaster/downtime**
  One or some hardware components within a facility are destroyed or disabled.

- **Application disaster/downtime**
  One or some software applications residing on hardware within the facility are destroyed or disabled.

- **Data disaste**r
  Data is corrupted or lost.

- **Network disaster**
  Data networks are compromised or disabled.

- **Security disaster**
  Company security for internal information is breached and data is affected (destroyed or modified).

Ask the Right Technology Questions

So how do you know if your disaster recovery plan is current and meeting management's expectations? "Disaster recovery" means different things to different people, but whether your definition focuses on system

Aspect

high availability, system recovery, or system redundancy, it's important to look at both the technology you have in place and the processes around that technology.

Before you can develop an effective disaster recovery plan, you need to answer these questions about your contact center technology:

- Is the system redundant within itself? Does it have redundant internal workings?

- Is full redundancy required in a disaster situation? (internal company decision)

- Can you run two systems, one primary and one backup, in two different locations?

- Can each of the systems (same location or not) be configured to handle the load for all transactions if one fails?

- Would the two systems share the load under normal operation?

- Does the system have a hot or cold standby if redundant concurrent systems are not desired/required?

- Does the hot standby system automatically start in the case of failure, or is manual intervention required?

- Can the cold standby system automatically/remotely be started in case of failure, or is manual intervention required?

Build People and Processes into the Plan

It's not enough though to have just the technology backed up. You also need to have processes in place for every possible type of disaster. For example, do your contact center employees know what do if business continuity is interrupted? Do they know where they should go to work, or if they have access to hosted applications that allow them to access contact center applications remotely from undamaged locations? Will there be agents in other geographic areas who can log in and service the affected areas? Are new self-service applications required to free up agent resources for critical matters required? Are scripting applications in place, and up to date, to allow for uniform customer service in case agents have to temporarily take on unfamiliar roles, and have agents been made aware of this possibility? Is someone charged with ensuring that your voice self-service options are automatically updated? Are CRM applications in place that will allow access to uniform customer information, and have the agents been trained to use the applications?

Many contact center vendors have seasoned consultants who can provide you with guidance on how to manage redundancy or failover and recovery processes, as well as recommend technology designed to handle excess capacity. Initially, consultants will work with your organization to document and categorize all of the contact centers and services your organization provides and determine the impact a disruption will have on those systems. Specifically, they will look at the cost of redundancy and fail-safe systems versus the mission-critical value of your centers. Naturally, some companies' centers are not as mission critical as others, so each company needs to decide if the cost has a valid return on investment.

Terminology

Hot Standby
A method of redundancy in which the primary and secondary (i.e., backup) systems run simultaneously. The data is mirrored to the secondary server in real time so that both systems contain identical information.

Cold Standby
A method of redundancy in which the secondary (i.e., backup) system is only called upon when the primary system fails. The system on cold standby receives scheduled data backups, but less frequently than a warm standby. Cold standby systems are used for non-critical applications or in cases where data is changed infrequently.

Next, the consultants will provide a recommendation regarding redundancy on each system, based on the suggested levels of recovery and the requirements around each of those systems.

In many cases, extra components or software may not be required because the existing component is covered under the recovery plans for hardware and/or software that the contact center already has in place. This can be determined during the discovery process.

The contact center should also be sure to coordinate its disaster recovery plans with the rest of the organization. There may be some overlap, and it is important not to assume that another area of the business is taking care of supporting the systems that overlap with the contact center.

Also, if you are outsourcing any portion of your contact center initiatives, you must be sure that the outsource vendor has its own recovery plans in place. Sarbanes-Oxley requires organizations to provide evidence of business continuity plans, and this includes vendor-provided services as well, including outsourced services.

Finally, the best disaster recovery plan is worthless if it isn't updated continually and tested regularly. All too often, call centers invest large amounts of time, money, and other resources into developing a plan but make the mistake of ignoring the maintenance required to keep the plan effective and efficient. The financial impact of relying on an untested or outdated plan can be devastating.

Natural and technological disasters can be business disasters as well—but they don't have to be. Businesses that proactively select and implement the appropriate disaster-recovery technologies and processes can keep disruptions in customer service to a minimum and keep revenue flowing in spite of unfortunate events.

About Aspect
Aspect provides software and consulting services that turn the potential of unified communications into real business results across the enterprise and in the contact center. Applying 35 years of insight and experience, Aspect helps more than two-thirds of the FORTUNE Global 100, as well as small and medium enterprises, power their business processes with communications. For more information, **visit www.aspect.com.**