

Protect Your Call Center With a Comprehensive Disaster Recovery Plan

Roberta J. Witty, Bern Elliot, Esteban Kolsky

The call center is a company's lifeline. Therefore, it must be available to customers and workforce constituents when an event forces the production environment out of service.

STRATEGIC PLANNING ASSUMPTION(S)

Through 2008, companies that prepare their customer service solutions for disasters, test them and implement them when needed will enjoy 40 percent greater customer loyalty (0.8 probability).

ANALYSIS

Call centers are fundamental to the life of a company. They play a mission-critical role and must be available to customers soon after a company crisis because service outages have a direct and measurable impact on company revenue and customer satisfaction. Loss of customer service and support can run into the millions of dollars per minute. Regulatory and corporate/competitive pressures are also forcing companies to develop effective recovery solutions.

Proactive companies should provide recovery with a tiered approach and they should test their plan at least once a year. In doing so, the company demonstrates its resiliency, thereby becoming more competitive and enjoying increased customer loyalty. Here, we answer some of the most frequently asked questions about call center recovery that we receive from clients.

What makes call center recovery different from other recovery problems?

When developing strategies for call center recovery, planners must first understand that a call center is often structured as an independent business unit within the company. Many times, call centers don't have a clear single owner in the IT organization. These individuals tend to be business application owners with infrastructure support needs that cross more than one IT group — including network, telecommunications, application development and testing, support, and the help desk. As a result, call center owners often have to go to the CIO and other senior managers to cover all aspects of recovery.

In many companies, multiple call centers serve different functions — some support inbound and outbound sales, others support a range of customer groups. Still other call centers provide internal support for HR and IT, or for product-support help desks. Centers also come in different sizes and configurations, with a variety of technology deployments needed to match the specific applications that they support. Some centers may have more than 1,000 agents networked across multiple physical sites, while others may have only three or four agents. Often, centers in the same company may be operated independently, with their own separate equipment vendors, applications and internal stakeholders. Each call center will also have a different level of criticality to the enterprise. Some centers, such as those in a hospital emergency center, directly affect people's lives. Others may strongly impact the success and failure of a company. Some call centers offer noncritical functionality that can be suspended for several days without seriously influencing company operations.

Because of this complex and broad set of constituents, environments and responsibilities, contact center recovery planning should not be considered a single monolithic problem. Each center in the company should be identified and its relative requirements and services categorized. This enables the ranking of each call center and service according to its importance, as well as better sharing of back-up resources — for instance, a critical center could temporarily use the resources of a noncritical one.

What is the best way to develop a call center disaster recovery plan?

The starting place is to document and categorize all the call centers and services in the company and assess the impact of disruption on each of their services. For each service, you must understand the primary business functions and the operating requirements.

For each service identified, an impact assessment for loss of services must be defined. This impact can be defined in terms of tangible and intangible cost. Some services are more critical than others. Those with major cost or liability exposure would have the highest rating — for instance, a hospital emergency call center. Other services, such as outbound telemarketing, would have a much lower impact rating. This forms the basis for developing general recovery time frame objectives (RTOs) for each service. Most call centers offer more than one service and you should not assume that all the services, even within a single center, are equal. Because some services are more critical than others, companies will use a tiered RTO for each service, based on its criticality. Time frames will vary from zero to several days or even weeks.

After each major call center and its services have been identified, the dependencies for operating each service — such as the systems and people involved — are identified. A series of risk statements are developed that describe each service-affecting cause or event. A risk statement defines a cause or event (for example, a power outage), an effect on a dependency (for example, the loss of a system) and a likelihood of occurrence (a scale of 1 to 5 in which 5 is very high risk). Gartner advises that companies use scenario planning to understand how various events will cause failures of components or the loss of individuals fulfilling roles. For convenience, dependencies can be divided into four major areas: IT (such as systems, applications and data networks), telecom (such as telecom systems, voice networks and carrier services), personnel (such as agents and supervisors) and facilities (such as buildings and power).

The result should be combined in a risk table. Each row in the table includes:

- Service (from call center) — for example, Tier 1 customer support; 100 agents
- Cause/event (from the risk statement) — for example, power failure
- Effect on a service dependency (from the risk statement) — for example, loss of all systems
- Likelihood (very low, low, medium, high, very high)
- Impact (very low, low, medium, high, very high)
- RTO — for example, less than five minutes
- Steps to mitigate/eliminate — for example, uninterruptible power supply (UPS)
- Cost to mitigate/eliminate — for example, the cost of a UPS and maintenance
- Other methods to mitigate/eliminate — for example, switch traffic to other site

The set of events considered in this risk table can start small, taking into consideration only the most-significant services and events. Over time, the table can be expanded to provide more detail.

How do voice over IP (VoIP) and IP telephony technologies change call center disaster recovery plans?

VoIP technologies offer the advantage of being distance-insensitive. That is, you can support remote agents and voice systems more easily than with alternative approaches. It is also easier to redirect voice traffic. This results in a wide range of new options for eliminating or mitigating various service-affecting events. VoIP technology can be used to provide new disaster recovery solutions in three areas.

Using VoIP to support redundant sites. VoIP can support agents in locations distant from the physical automatic call distribution (ACD). The ACD can be located in a highly secure facility,

while the agents themselves are located in multiple physical sites. The result is that a storm or other problem that affects one location will not affect the others, thus the service is not interrupted. Additionally, a back-up switch can be deployed in a different location. With two sites for agents and switches, the problem of a "single point of failure" has been eliminated.

Using IP technology to support work-at-home (WAH) agents. Agents can be set up with high-speed Internet at their homes. In the event of a disaster that keeps agents from traveling to work, the agents can log into the work system using remote access technology. They can configure their agent logon profile so that calls are sent to their home phone or, in some cases, to a desktop softphone. In this way, agent services can continue despite a disaster.

Using VoIP for network-based resources. Many contact center systems, such as ACD, computer-telephony integration and interactive voice response can be located at a service provider facility. The company uses these systems as if they were on their own premises, including Web administration and reporting. Because the systems are network-based, they can more easily address disaster recovery requirements. Calls are then handled and routed from the carrier's network. This also enables support for agents at multiple locations.

What is the effect of WAH agents in a contact center disaster recovery plan?

WAH agents have been growing in popularity during the past 12 months, due to the availability of broadband access, their own availability in short-time and on-demand situations, and the reduced costs of running a call center with employees who work from home. In addition, these employees are more motivated, work more effectively and reduce churn to very low levels. Another benefit of using WAH employees, and one that directly involves disaster recovery planning (DRP), is that they can be spread across several geographic areas. These WAH employees can provide coverage at odd hours or at critical times — such as when a disaster strikes in a specific location. If, for example, an earthquake occurs in California, WAH employees in different regions can be called to action to cover for those affected by the earthquake. In planning to use WAH agents for DRP, consider these factors:

Infrastructure location. If the application, the communication infrastructure or the data necessary to answer questions is located at one site without replication, and that location goes down, it will be impossible for employees to do their job properly.

Skills and personnel management. Workforce management software is necessary to ensure that the right WAH agents are deployed at the right time and can provide the right answers. This software provides skills and time management, scheduling, scenario planning and notification — functions that are essential to bring the call center back to work with the disparate resources that may be available.

Compliance considerations. Even during emergencies, federal, state and local compliance laws remain in effect. Organizations looking to use WAH agents in the event of DRP should understand the compliance implications and plan accordingly via training and resources. Otherwise, exclude specific compliance-dependent functions from DRP; that is: 1) functions performed by agents who may lack required training or certification or 2) actions that may require the sharing of data that compliance requirements deem to be not sharable. For example, if you are located in a state in which only certified financial planners (CFPs) can deal with financial information, and your WAH agents aren't CFPs, you cannot include these functions in the DRP.

How do contact centers manage disaster recovery plans?

It is inaccurate to say that contact centers are completely different from call centers. Contact centers deal with the same issues as a call center, but they compound them by several channels (as in e-mail, Web chat, and potentially Short Message Service and instant messaging). When

talking about DRP for a contact center — which may or may not include call center functions — follow three steps to determine the appropriate actions to take:

Determine the need for each channel. For each organization, each channel will be implemented differently and have a different value. For example, no organization should assume that e-mail is critical to its operations. Instead, question business units and end users about the channel and its functions, or analyze operations for the preceding 12 months to determine the need for the channel in case of disaster.

Determine the feasibility. For example, if a disaster took down the Internet, it would not be possible to provide services via e-mail, Web self-service or chat. If the need for e-mail is critical following a disaster, perhaps a separate method for providing e-mail should be evaluated (such as a private network or alternate methods like pagers or cellular phones — as long as they use different networks).

Co-ordinate with other discovery recovery plans. It's likely that components in other areas of disaster recovery or even in the call center disaster recovery plan can be leveraged into other channels. For example, if a call center DRP calls for the use of a private network for VoIP or a similar form of communication, an e-mail DRP could leverage that network to transmit e-mail and, if necessary, could include customers and partners in the network to enable them to continue operations. These actions underscore the point that contact center planning, as well as the call center, should not be seen as separate from the rest of the organization. Rather, the contact center should be considered critical to the operation of the organization and be included in the companywide planning project.

Key Issues

What strategies, programs, disciplines and best practices will enterprises employ to improve their resilience in the event of a disaster?

Acronym Key

ACD	automatic call distribution
CFP	certified financial planner
DRP	disaster recovery planning
RTO	recovery time frame objective
UPS	uninterruptible power supply
VoIP	voice over Internet Protocol
WAH	work at home

This research is part of a set of related research pieces. See "Use Good Business Continuity Management to Prepare for a Disaster" for an overview.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509