

LEVERAGING TECHNOLOGY TO OPTIMIZE CONTINUITY AND RECOVERY

Reduce your risks and position your center to take care of customers...
no matter what happens.

By **Matt Morey and Ken Barton**

Strategic Contact Inc.

 @StratContact



Matt Morey is a Senior Consultant at Strategic Contact

matt@strategiccontact.com
(913) 681-5133



Ken Barton is a Consultant at Strategic Contact

ken@strategiccontact.com
(954) 942-3598

Ever have a nagging feeling that your center is more vulnerable than you'd like to admit? Odds are, creating or updating that dreaded business continuity/disaster recovery (BC/DR) plan has been on your "to do" list for some time. Today's technology and service offerings provide new options to address risk reduction and just may change your perspective on (finally) addressing your BC/DR strategy.

Getting the BC/DR Ball Rolling: Look at Scope, Costs and Options

The first order of business when preparing and/or assessing your BC/DR plan is to determine how far to go in terms depth and breadth. To do so, you'll identify relevant risks, the likelihood of their occurrence, and the associated business impact. You'll consider how long you can reasonably tolerate an interruption—e.g., minutes, hours or days. Then you'll define your levels of risk mitigation. Categorize the likelihood of each risk occurring and the associated impact (see Figure 1). Knowing how each risk and impact affects your operation helps you determine the level of redundancy to build into your overall architecture from a network and system perspective.

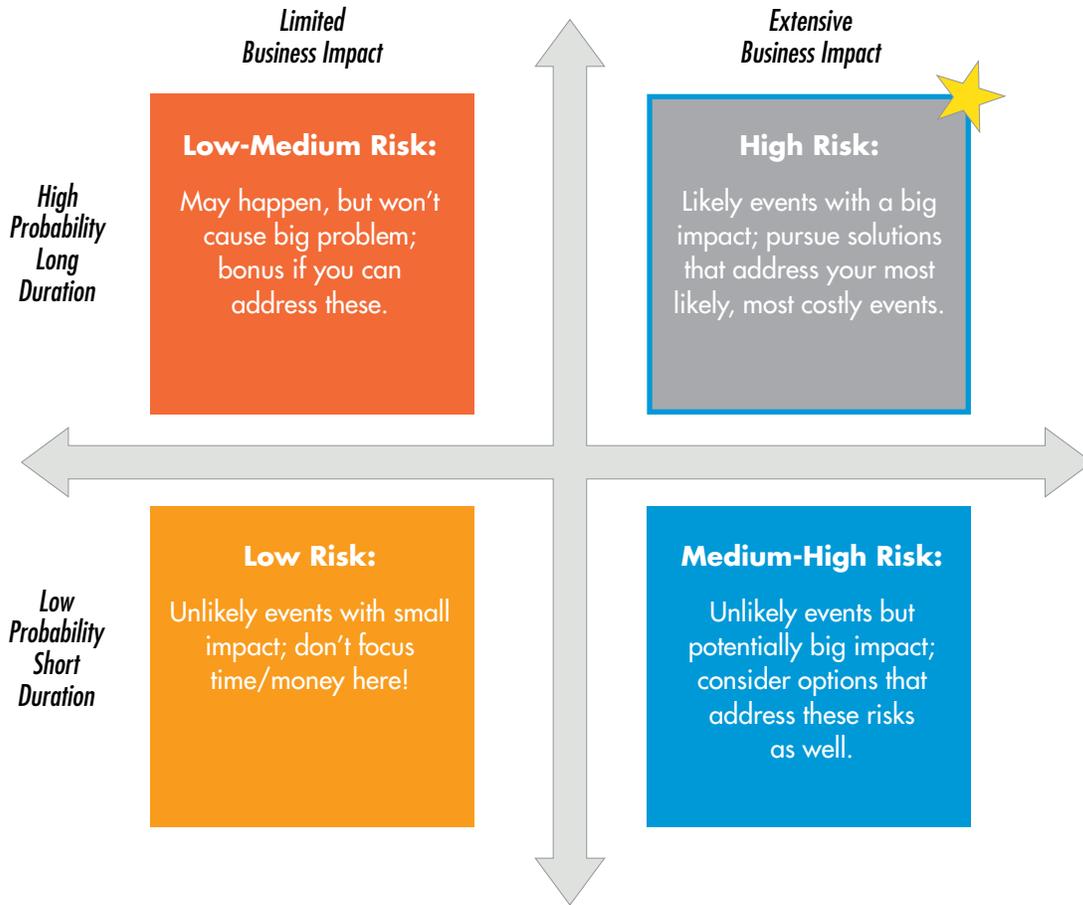
Natural disasters are the obvious starting point when defining vulnerabilities. Hurricanes, tornadoes, earthquakes, snow storms and floods can significantly impact your business. You'll want to identify alternate location strategies where agents can handle contacts in the event your building is inaccessible, and make sure they can readily access your systems when they get there. Beyond Mother Nature's threats lie other risks:

- While redundancy can protect you from hardware or software failures, there are no guarantees. A technology failure can limit functionality, customer access and/or center performance. This category is a big one, so list the elements of your infrastructure and applications and the things that can go wrong, and define your options to address them.
- Are you prepared for construction equipment severing a cable or other network outages? Consider multiple data centers and/or access points with diverse routes into your data center(s) in the event your main access is disabled.
- What if you lose power? Review your backup power approach and ensure that you know exactly how long you can operate, then look at options such as generators to increase resiliency, if necessary.
- Are you prepared for employee illnesses or a pandemic? You may need plans—and technology in place—for non-contact center employees to handle simple calls or look to an outsourcer or remote or home agents to cover your bases.

Take a look at these types of scenarios (and others on your list) and assign a rating of likelihood. Then you can prioritize the highest risk situations.

Now you are in the position to assess the scope of your plan and truly examine the costs of your BC/DR options. You'll need to determine the financial impact to the business and the cost to support different configurations and aspects of the plan from operational and technical perspectives. Start with identifying and addressing single points of failure. Typical single points of failure include network access points to your facilities and hardware (e.g., routers, gateways and servers). Next, you will want to consider the operational side of delivering calls to your agents. For each scenario, you need to consider if you can get enough people in the right place at the right time, with access to the right systems, and the costs of doing so.

FIGURE 1: Categorize Risks and Impacts



Many multisite centers' BC/DR plans include adding seats in unaffected sites by placing agents in training rooms, conference rooms or other areas. They build sufficient network capacity in advance and have work stations available and configured to quickly place in the temporary locations. Some offsite data centers can provide expanded space for hardware and seats as well as added capacity. Some data centers even provide agent stations already wired and set up for use just for DR purposes. Many data management services vendors assist with data backup and recovery, which should be considered in your plan. Outsourcers sometimes offer space for your agents in addition to their own agents answering your calls.

Each of these scenarios can have an impact on hardware, software and network capacity requirements. Consider the number and types of seats you need for business continuity, including agent, supervisor and support staff, and the bandwidth demands when contacts are diverted.

Times Change and So Does Technology

The past decade has given way to a number of new technologies to support the scope of your BC/DR plan. These new technologies include cloud services, server virtualization, mobile computing and social networks. While you may want to consider any or all of these developments, cloud services are a great place to start. Your cloud vendor can provide complete contact center technology solutions at their data centers or backup to your premise solution



SUBSCRIBER DOWNLOAD:

“Win! Win! Win! The Cloud Contact Center Has Something for Everybody,”

» bit.ly/1wBASHq

in the event of a disaster. When using cloud services, you can secure service level agreements for performance that includes uptime (see “Win! Win! Win! The Cloud Contact Center Has Something for Everybody,” *Pipeline*, December 2012).

If new cloud contact center technology has spurred your BC/DR rejuvenation, make sure that the services you are considering are BC/DR-ready for your environment. Top items to address are:

- Ensure that your vendor supports the proper network access and application configuration for your routing and reporting.
- Negotiate SLAs for uptime.
- Determine how calls will be routed in BC/DR mode.
- Understand the processes for transition and the impact on the customers.
- Define multiple ways to contact your cloud vendor in the event of a disaster and the process for initiating switchover.

Server virtualization is another technology development that makes it easier to support your BC/DR plan from a hardware perspective. Using virtualized servers results in a smaller footprint, which is easier to maintain as it requires fewer boxes and can lower your overall total cost of ownership. Place virtualized servers in geo-redundant data centers to bolster your survivability.

Mobile computing and BYOD (bring your own device) enables your contact center resources to work remotely in the event you need to implement BC/DR measures. These options give you the flexibility to quickly open a center in nearly any unaffected location using cell phones, tablets and/or laptops. You may not have access to your full back-office applications and may not handle interactions using the most efficient processes, but at least you are answering the calls and responding to emails. This could be a very viable alternative to hold you over until your backup location is set up and ready to go.

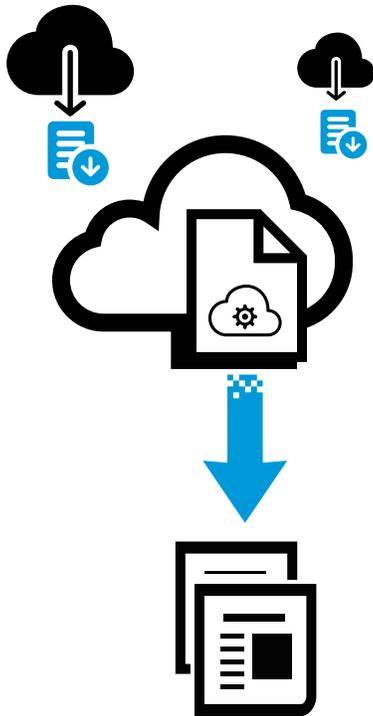
Social media and SMS texting expand your lines of communication with your employees, if an event should occur. You can quickly inform employees what BC/DR measures have been put into place, where they need to be, and what next steps are. The bonus: These technologies are not reliant on your corporate communications systems (that may be down if you are enacting BC/DR measures).

Don't Forget Documentation and Testing

Documentation and testing processes for BC/DR continue to evolve, as well. From a documentation perspective, many folks simply distribute plans in binders, which can be a challenge to keep current. Enter the cloud again: You can store the plan electronically in your own systems as well as third-party cloud storage. Keep paper copies to accompany the electronic version and be sure that employees know how to quickly access the plan.

The keys to success in documenting the plan are to be thorough while keeping it as simple as possible. Then, put it to the test. If you can't successfully execute a test run, your design is too complicated or documentation unclear. But also realize a solid BC/DR test involves more than simply your IT department testing your technology. A BC/DR plan is of no value if corresponding operational plans are not in place, aligned, updated and tested for all personnel (IT and CC).

Test your BC/DR plan on a regular basis. The level and frequency of testing varies with the scope of your plan, your vulnerabilities and risks, and your budget, but once a year should be the minimum. Test the network, access and technology. Test call routing and access to data in the telephony and back-office systems. If utilizing alternate sites or outsourcer services, be sure to test transitioning contact routing to these locations and restoration when things are “back to normal.”



Testing should encompass the operational side, as well. Does your staff know what to do, where to go, how to get there, and what to do when they arrive? Test how people will get to the right place at the right time in the alternate sites. Test all your communication methodologies: IVR messages, social media, SMS texts, etc. Clearly identify responsibility from a program management perspective. Know who executes the overall plan and who is responsible for specific areas and tasks, including primary and backup resources. Work with and get to know your vendors and how to contact them for their assistance in execution of your plan. You never know if your plan is going to work unless you test it!

The scenarios that you identified as high impact and high probability when you conducted your risk analysis should be first on your list to test (see Figure 1). Be sure to revise and adjust processes and documentation as necessary based on testing outcomes and reviews of how technology and staff performed. Additionally, it is imperative to clearly define the “owner” of updates, maintenance, and distribution/communication of the plan. That role should include updating based on new technology configurations and processes, as well.

The First Step Is the Hardest; Start or Update Your Plan Today

If your organization currently doesn't have a BC/DR plan, it's time to get started. If you currently have a BC/DR plan, maybe it's time for an update. Consider how technology changes can help you fine-tune your plan. Technology additions and improvements provide a nice counterbalance to the nagging feeling that we are more vulnerable than ever. It's time to reduce your risks and position your center to take care of customers no matter what challenges get thrown your way. 🌐

WHAT THE "BEST" CENTERS DO FOR BC/DR

Use this checklist to align your contact center with best practices, and ensure that you are ready for continuity and recovery when bad things happen.



- Define a strategy for BC/DR that considers vulnerabilities and impacts.
- Consider that BC/DR strategy in all technology requirements, purchases and design efforts.
- Make the appropriate investments to mitigate risks and be prepared to act when events occur.
- Build resiliency into architectures through things such as geo-redundant data centers, diverse network routing, high-availability solutions and routine backups.
- Develop detailed and thorough BC/DR plan(s) that address technology and operations.
- Test BC/DR scenarios routinely (e.g., twice a year) from start to finish, including restoration of normal operations, with IT and business leader involvement.
- Leverage technology advances to improve BC/DR execution.
- Update BC/DR plans routinely based on changes to systems or processes, new capabilities, test results or other factors.

About Contact Center Pipeline

Contact Center Pipeline is a monthly instructional journal focused on driving business success through effective contact center direction and decisions. Each issue contains informative articles, case studies, best practices, research and coverage of trends that impact the customer experience. Our writers and contributors are well-known industry experts with a unique understanding of how to optimize resources and maximize the value the organization provides to its customers.

To learn more, visit: www.contactcenterpipeline.com



Online Resource

This issue is available online at: [ContactCenterPipeline.com](http://www.contactcenterpipeline.com)

<http://www.contactcenterpipeline.com/CcpViewIndex.aspx?PubType=2>