

The Most Overlooked Component of Business Continuity



July 31, 2018 / Peter Eisengrein

Business leaders meticulously plan for future growth and expansion but are often caught off-guard by disasters. Local storms, fires, power, and network outages continuously wreak havoc on organizations, meanwhile, large-scale disasters seem to be increasing in intensity and quantity. 2017 was a perfect example of the top three costliest weather-related disasters to hit the U.S. and its territories, at \$125 billion, \$50 billion, and \$90 billion, respectively.

Unfortunately, survey data shows that business leaders tend to believe they're better prepared than they actually are, as they typically don't have a granular view of their technical capabilities to resume business after an incident. This misunderstanding can greatly harm a business's ability to resume operations quickly. In fact, 25 percent of businesses do not reopen following a major disaster according to The Institute for Business and Home Safety.

While IT leaders are generally prepared with solutions to get servers and data centers up-and-running quickly, *business continuity for communications capabilities is often overlooked*. That oversight can cause significant financial damage as customers that are unable to contact a business is likely to look or purchase elsewhere. Additionally, the reputational damage caused by the inability to communicate with a business can sometimes play a heavier role in the organization's failure than any other factor. Further, lost communication services also disrupt the ability of staff members to collaborate and for partners to meet supply chain deliverables.

Preparing for the Worst: Developing a Business Continuity Plan for Communications Systems

For all organizations, the first step in business continuity planning for communications systems is to better understand your financial exposure. [Calculate the cost of downtime](#) for your organization from

every perspective. While every business is different, Gartner estimates that for some businesses downtime can cost \$5,600 per minute and as much as \$540,000 per hour in more extreme scenarios.

Business Continuity for On-Premises Communications Systems

For businesses with phone systems that reside on-premises, a local disaster can effectively disconnect that site from the rest of the world. Therefore, it is critical that a business decides which functions to restore first. Consider key business operations – from customer-facing units to human resources – and understand how IT and telecommunications systems are needed to support each function. It can be helpful to visually map continuity priorities, lines of jurisdiction, areas of primary business concern, and the order in which systems will be restored in the event of a disruption.

Additionally, ensure the following are completed:

- Prepare a checklist of key telephony vendors to manually re-route calls to enable alternative ring-to locations and numbers (if possible) and designate emergency personnel to take and triage inbound calls.
- Create a written recovery plan that is stored remotely. Make sure you have written methods of procedure to support the plan so that someone unfamiliar with the tasks can step in to handle it in the time of need. Make sure this information is available remotely and does not exist solely at the location, in case it is unreachable.
- Build a list of key employee contacts for each department that includes mobile and home numbers along with alternate email addresses.
- Identify vulnerabilities in your physical facilities, IT infrastructure and communication systems. This might include single points of failure in systems for:
 - Internal networking & connectivity
 - Service providers
 - Power
 - Hardware/systems, service providers, etc.
 - Consider what would happen if any one of these things failed!
- Manage and test physical safety systems for fire, smoke, and flooding. Maintain your fire suppression systems and have them inspected on schedule.
- Plan and build extensive cooling and ventilation systems. All the system redundancy in the world doesn't matter if the equipment overheats; have these systems regularly maintained.
- Purchase uninterrupted power supplies (UPS) and generators. Make sure mission-critical systems are supplied by your backup power. Perform periodic power outages – *you don't want to find out in an emergency that the system doesn't actually power your phone system, or that the POE switches that power the phones are not on backup power.*
 - Also, make sure your UPS and generators are sized correctly. If not, systems may not stay up as long as you thought. Or worse, you overload the backup and cause it to fail.

- Make sure you have sufficient fuel for the generator. In a real disaster scenario, it may be days before you can fill up. And if you don't have a generator, identify and contract ahead of time with a company who can bring in a portable generator on a truck, and have a certified electrician pre-install the necessary cabling for a portable generator.
- Schedule nightly backups of all mission-critical systems, and weekly backups of the rest. Make sure the backups are not stored on-site with that equipment. Regularly audit that the backups are actually happening and periodically test restoring from backup, at least annually.

How Disaster Recovery for Cloud Communications Is Different:

Regardless of conditions on-site, cloud-based unified communications (UC) systems answer inbound calls, forward callers to voicemail, or automatically reroute calls to a cell phone. Even when a business location is unavailable for an extended period of time, staff members can seamlessly continue business operations via a soft client to remain productive without customers knowing they're "homesourcing."

Because of these inherent capabilities, for an increasing number of businesses, cloud-based voice, video, and instant messaging services have become the go-to method for ensuring communications business continuity. In fact, [our recent survey](#) noted that 30% of North American businesses would be evaluating a cloud communications system.

As you might expect, because of the lack of onsite equipment business continuity planning is significantly streamlined in a unified communications environment. On-premises equipment requirements are usually handled by the service provider, often with significantly greater security and backup measures put into place. For example, at Evolve IP our cloud communications platform is:

- Deployed across multiple SOC 2 geographic data centers (located in the world's most secure locations like SWITCH, Las Vegas).
- Within each location Evolve IP ensures system and application-level redundancy.
- In the highly unlikely event that an entire data center were to go down, services transfer instantaneously to a mirrored site hundreds or thousands of miles away.

Cloud service providers generally also leverage a highly diversified network connectivity architecture to ensure uptime. At Evolve IP we actively monitor and route voice traffic with 12 of the world's top providers (like Verizon and CenturyLink) across over 120 global routes. In addition, we have differentiated data connectivity capabilities via 20 different internet service and private connectivity providers.

As with on-premises, you should also employ multiple Internet providers in your location and test for failover regularly. Or, better yet, deploy an SD-WAN service like Evolve IP's Cloud Connect so that your network stays up, even if one, or even more, providers do not.

So, essentially, in a cloud communications scenario businesses need only to:

- Identify which communications channels (email, toll-free lines, contact centers, VPNs, Terminal Services) are most vital.
- Determine who needs secure access to these systems.

- Deploy internal communications.
- Engage disaster playbook procedures e.g. pre-defined routing/forwarding rules, messages/alerts, remote work policies.
- Continue business as usual until the site becomes operational.

Other Benefits of Cloud Communications

1. Cloud-based unified communications systems also help businesses more easily scale, grow and expand. In a UC environment, adding new locations, extensions, departments, and resources is simple, and each site is easily managed in the event of a disaster.
2. UC systems also present a number of financial advantages. The cloud-based subscription model is a predictable operational expense, whereas maintaining an on-site PBX is a significant capital expense with ongoing (and often prohibitive and unpredictable) maintenance costs.

More than ever before, businesses are exposed to a wider array of potential business disruptions. Whether a disaster is caused by natural causes, a cyber attack, employee-sabotage or any number of other issues, business continuity planning is the key survival. Regardless of cloud or on-premises architecture, your business should allocate the time and resources to update your recovery and continuity plans to include your communications systems today.