

---

**CONTENTS**

---

- 2 Quantify the Cost of an Outage
  - 3 Potential Types of Outage
  - 4 Develop a Plan
  - 8 Conclusion
- 

# Disaster Prevention, Not Disaster Recovery

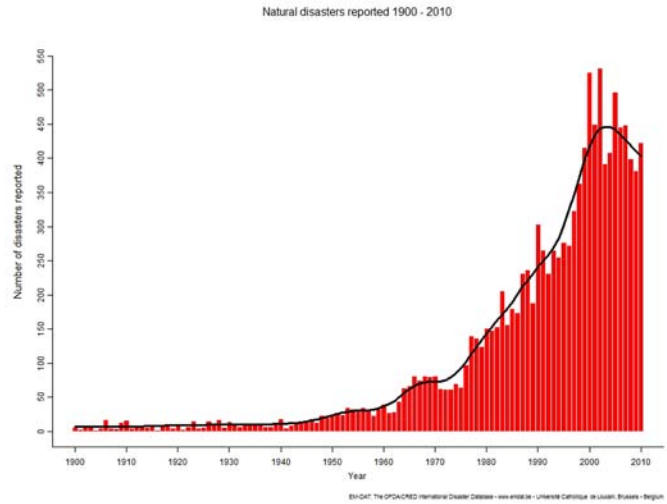
Vertical Communications, Inc.  
Published December, 2011

Planning for outages and emergencies has always been difficult. Many businesses are unsure how to proceed. How much money should be spent? What are the possible threats? Do I need this? Today, businesses around the world face increased potential for disasters that will stop their daily operations, but aren't sure how to handle it.

This document outlines a proven methodology for avoiding disaster scenarios through proper engineering of your telecommunication systems and preparation ahead of time.

## Quantify the Cost of an Outage to Your Organization

Disaster recovery planning tends to start by listing potential threats. Disaster prevention starts with determining the cost of a disaster to your business. Disaster planning can often seem like a bottomless hole into which you can never pour enough money. No one can prepare for every disaster possibility. The smart business decision is to evaluate the real cost to your company of a system outage.



Natural disasters reported 1900-2010 - International Disaster Database ([www.emdat.be](http://www.emdat.be))

### STEP 1: Evaluate the Cost of an Outage

A. *Determine the average value of each call.*

Each business communication is generally either helping to generate a new sale, closing a sale, or delivering the sold service or product. You need to evaluate the average revenue of each type of business transaction and use that to the impact to your company in lost sales, lost customers, and other costs in the event of an outage.

B. *Determine the number of missed calls.*

You need to know how many calls your business is making and taking and what kind of calls each of these are. Detailed call logging and the ability to annotate calls and/or record calls are key capabilities to making this happen. Without these abilities, you can't even begin to plan. With them, you can estimate a dollar amount that an outage would cost you.

	10 minutes	1-2 hours	1 day	3 days+
Number of communications				
Average revenue/communication				
Total Estimated Outage Cost				

## STEP 2: Establish Representative Outage Lengths to Plan Against

- A. 10 Minute Outage
- B. 1-2 Hour Outage
- C. 1 Day Outage
- D. 3 Days or more Outage

We recommend looking at four lengths of outages: 10 minutes, 1-2 hours, 1 day, and 3 days or more (the commonly cited statistic is that 40% of companies which shut down for 3 or more days will fail completely within 36 months<sup>1</sup>).

## STEP 3: Determine the Likelihood of an Outage for Your Business

### *Option 1: Conduct a detailed risk analysis*

A detailed risk analysis using an outside consultant or insurance company will provide very accurate information. It is very expensive and time-consuming though. You may not have the resources to dedicate to it. A sample process can be found in the online Disaster Recovery Journal, [http://www.drj.com/new2dr/w3\\_030.htm](http://www.drj.com/new2dr/w3_030.htm)

### *Option 2: Use the rule of thumb method*

A simple rule of thumb is to plan for a disaster occurring every 24 months. This rule is based on a Veritas report surveying companies worldwide in 2004. 51% of companies surveyed had executed their disaster plan in the previous 12 months and only 18% had never executed their disaster plan<sup>2</sup>. This allows you to look at the numbers you have compiled for cost and estimate they are likely to come due some time within the next two years. If you plan instead to spend 25% of that cost over the next two years on disaster planning, you will have a good budget to start with.



*Joplin, Missouri, May 22, 2011 - An EF-5, the most powerful tornado possible, destroyed nearly 7,000 homes, businesses and schools.*

## Understand the Potential Types of Outage

Disaster recovery planning focuses on causes. It requires listing every possible way that an outage can occur. Just creating the list is a daunting task and often causes the failure of many disaster planning projects.

<sup>1</sup> 2001 Cost of Downtime - Eagle Rock Alliance, "Contingency Planning and Management"

<sup>2</sup> The VERITAS Disaster Recovery Research 2004 - Dynamic Markets 2004, [http://eval.veritas.com/mktginfo/products/White\\_Papers/High\\_Availability/dynamic\\_markets\\_executive\\_summary.pdf](http://eval.veritas.com/mktginfo/products/White_Papers/High_Availability/dynamic_markets_executive_summary.pdf)

Our Disaster Prevention methodology focuses on results. We have identified the four types of outage that result from the huge variety of causes. Threats are unlimited, but they cause only four types of outage. Disaster prevention focuses on results instead of causes, making planning simpler.

### **Site Outage**

This type includes any threat that prevents your business site from being used. Common threats that cause a site outage include power outages, weather (snow storms, hurricanes, floods, etc). Regardless of the cause, business must be conducted at a different site.

### **Access Outage**

When your site is up, but personnel can't get to it, you have an access outage. A snow storm, a widespread flu epidemic, a chemical spill that has evacuated your building; all of your systems are up, but the staff isn't where the systems are.

### **Carrier Service Outage**

	Site Outage	Access Outage	Carrier Service Outage	System Outage
Solution	Reroute calls to off-site resource	Reroute calls to off-site resource	Reroute calls to off-site resource	Reroute calls to off-site resource

The internet or phone line connections are not available. This might be a carrier issue, equipment failure, or some other issue. The net result in all cases is that you cannot make or receive phone calls.

### **System Outage**

This is when your actual equipment, is down. Maybe a power surge fried equipment, a network virus attacked the system, or a component just failed. The system is out.

## **Develop a Plan to Address the Results**

In disaster recovery planning you must address what to do when each threat occurs. This is costly as each solution to recover from a potential threat is generally unique. Focusing on power outages means buying battery backups, generators, or even dual power feeds. Each solution only fixes one problem.

By focusing on the results rather than the cause, we only have to plan for four possibilities. If we examine those four outage scenarios, we see that all of them can be solved by a single solution.

A single solution is a very good thing for budgetary purposes. Rather than dividing your disaster planning budget into different projects each only useful to solve one cause, our disaster prevention scenario can put all of its resources into a single solution that addresses the results.

## **Single Solution: The Off-Site Resource**

This single solution can solve all of your disaster problems. Focus your Disaster Prevention planning on developing an effective off-site resource for handling all of your telecommunication needs. This resource may take several different forms depending on the budget you developed in our first step.

### **Second Site Routing**

Customers who have multiple sites can use Vertical's multi-site solution. When one site has an outage, the carrier can reroute call to another Wave location. A pre-planned configuration maximizes use of available resources to handle the emergency load.

### **Off-Site System**

For business who only have one location, the next solution is a Wave system. This system can be installed off-site in a data center with your other critical systems. The system can take over calls in the event of a disaster. The Vertical Wave IP® system uses Mobile Extension technology to allow users at any phone to take calls just as if they were in the office. Calls can be logged, recorded, and controlled, just as if the user was at their desk. Call centers can still function with users at remote locations.

### **Backup Site**

A Vertical system can also be put in place at a full-fledged backup site. Such a site needs to be geographically separated from the primary site, but easily accessible within a short amount of time. This site can use service such as usage only SIP trunks to minimize its continuing upkeep costs. This is the most expensive option as the business will have to pay for the backup site, duplicate equipment, and other ongoing costs. However, it will allow maximum effectiveness in the event of a disaster. If your potential risk is very high, then this option may be for you.

## **Single Solution - Planning**

No matter which option you choose, you must develop a plan to make this solution work.

### **Phone Number Redirect**

Regardless of which option you choose, inbound calls must be redirected from your primary site to the backup site. Many carriers refuse to provide timely rerouting of calls in the event of a disaster, much less automatic rerouting. Finding a carrier that provides this service is the key to successful planning. This is one of the key advantages to SIP trunking services. SIP providers can provide trunks that can be instantly switched to any backup location with appropriate internet service. This eliminates the need for backup phone service in two places in the case of hosted or backup site solutions. Whatever method used, it is critical that you have a method for rerouting your phone numbers to your off-site resource.

## Call Routing

Once the calls have been redirected, you need to plan how they are handled at the receiving end. This will be different than your main site (unless you have an identical backup site). The key is to sit down with your certified Vertical solution provider and make a plan. They will then implement the configuration based on that plan. The plan should consider:

- Will you alert callers to the emergency situation (setting their expectations)?
- How will your call routing change?
- Where will you send the calls (remote users using Mobile Extension, another site, answering services, etc)?
- How will you log and track the emergency calls?

## Responsibility

A critical part of the planning process is assigning responsibility.

- Who decides when it must be implemented?
- Who is the backup person in case the disaster affects that primary person?
- How is the plan implemented?
- Is it automatic or does someone have to decide to make the change?

Why not redundant systems?

The most common backup solution is a live backup system, a hot-spare. Why do we not recommend this?

Two reasons:

- Hot-spares only fix one outage type (System Failure)
- Hot-spares are exposed to all of the likely failure causes (power, environment, network)

A hot-spare will likely be unusable just like the primary system!



*Consider placing your backup site in a safe area with minimum risk*

During a disaster is never the time to make these decisions. To make sure you achieve disaster prevention, outlining who is responsible, who their backup is, and how they will implement changes is key. Which brings us to the final planning step.

### **Document the Plan**

Documenting means more than just writing down the plan. It includes:

- Make multiple copies to a disaster doesn't take out the documentation
- Make those copies easily accessible for all circumstances
- Making sure all key parties have read the plan
- Update the plan regularly so it stays current

### **Single Solution - Practice**

A disaster plan will only prevent problems if it works. The only way to ensure that a plan works is to pull it out regularly and practice it. This ensures that everyone is familiar with the plan. It makes sure that the plan is up to date to current circumstances. It makes sure all of the systems actually perform. This means that a regular practice must be included in your disaster prevention budget.

Without regular practice, a plan is quickly worthless. The odds of it actually working decrease every day it isn't tested. The same study on disaster plans in companies mentioned earlier found that less than half of all companies that DID have a disaster plan had practiced it even once in the previous year<sup>2</sup>. That kind of behavior is a recipe for disaster!

Test your communications disaster prevention plan on at least a quarterly basis. This will guarantee that your solution will work and increase confidence throughout the company. The plan will be ready and practiced to prevent any disaster the affects your company and prevent costly outages.

---

<sup>2</sup> The VERITAS Disaster Recovery Research 2004 - Dynamic Markets 2004,  
[http://eval.veritas.com/mktginfo/products/White\\_Papers/High\\_Availability/dynamic\\_markets\\_executive\\_summary.pdf](http://eval.veritas.com/mktginfo/products/White_Papers/High_Availability/dynamic_markets_executive_summary.pdf)

## Conclusion

Disaster prevention is a reachable goal. It doesn't require huge amounts of effort with no return. If you identify the potential cost and structure your disaster prevention budget accordingly, then you can manage the cost of preparedness. Further reduce cost, by looking at the potential outages and developing a single solution to the four outage results rather than dividing your time and money trying to recover from hundreds of individual causes. Then, choose the right option for your company depending upon the budget assigned and the resources you have (such as multiple sites). Finally, you can develop a real plan with the help of your Vertical certified solution provider. With regular tests, you can prevent disaster rather than just recovering from it.

### Corporate Headquarters

3940 Freedom Circle  
Santa Clara, CA 95054  
USA  
Phone: (408) 404-1600  
FAX: (408) 969-9601

### Customer & Technical Support

4717 East Hilton Avenue,  
Suite 400  
Phoenix, AZ 85034  
USA  
Phone: (480) 374-8900  
FAX: (480) 374-8852

### Charlottesville

1180 Seminole Trail, Suite 150  
Charlottesville, VA 22901  
USA  
Phone: 1-877-VERTICAL  
(1-877-837-8422)  
Select Option 0 for a Dial  
by Name

### Europe

Vertical Communications GmbH  
EMEA Sales  
Domagkstrasse 7  
85551 Kirchheim, Germany  
Phone: +49 89 90779460  
Fax: +49 89 90779488

