

# Preparing for the Inevitable: Natural Disasters

A Guide to Creating a Comprehensive Natural  
Disaster Preparedness Program

Let's cut to the chase: natural disasters are inevitable. There may be state-of-the-art tools, technology and incredibly smart people to predict these events, but the truth is that we can never prevent them.

Whether you've seen it on the news or lived it first hand, you know how much damage and destruction a natural disaster can cause; they often have a very negative impact on the residents, communities and businesses that stand in its path of destruction. So, what can businesses do to mitigate the impact of natural disasters like floods, hurricanes or earthquakes? How do we keep our employees safe, while also minimizing the business disruption? How do we plan and prepare for a natural disaster to ensure a swift response and recovery?

You've come to the right place. Apart from having a psychic ability to predict the future, the next best thing is to have the plans, people and processes in place to respond and recover when a disaster strikes.

This eBook is an end-to-end resource that leverages business continuity and disaster recovery principles to help you create a comprehensive natural disaster preparedness program. It includes everything from the greatest risks, how to plan and prepare, the best practices for recovery and pivotal lessons learned from disasters of the past.



More than 40%

of businesses never reopen after a disaster, and for those that do, only 29% were still operating after two years.

And guess what becomes of those that lost their IT for more than 9 days?

Bankruptcy within a year.

## Table of Contents

Top Risks Associated with Natural Disasters	3
How to Prepare for Natural Disasters	5
3 Steps for Better Disaster Recovery	7
Lessons Learned from Hurricanes Harvey & Irma	8

## Terminology

### **Emergency Preparedness:**

The planning that a company engages in to plan and prepare for negative events.

### **Crisis Management:**

The steps a company takes immediately after a negative event occurs to protect company assets, including its employees and data.

### **Critical Business Function (CBF):**

Activities and processes that must be restored in the event of a disruption to protect the organization's assets, meet organizational needs, and satisfy regulations.

### **Disaster Recovery (DR):**

A set of policies, plans and procedures to recover or continue operating vital technology infrastructure and systems following a disaster. Also referred to as DR.

### **Business Continuity (BC):**

The process of creating systems, plans and procedures to ensure that an organization can continue operating after a serious incident or disaster, or can recover to an operational state quickly. Also referred to as BC.

### **Business Resilience:**

An organization's ability to adapt to disruptions while maintaining continuous operations and protecting people, assets and overall brand equity.

## Top Risks Associated with Natural Disasters

The first step in creating an emergency preparedness plan is identifying the greatest risks that a natural disaster presents to your organization. Also known as a risk assessment, the purpose of this exercise is to evaluate the likelihood of those risks and their impact on the organization's critical business functions. Once those risks have been identified, your organization can create plans that manage, eliminate or mitigate those risks.

So, what are the top risks associated with natural disasters?

### 1. Damage to Assets and Physical Property

This is obvious but probably the most prominent risk that businesses need to consider. When natural disasters strike, they often do substantial damage to physical assets. Company buildings and property may be damaged, or equipment could also be ruined.

### 2. Damage to Raw Materials

Natural resources are another direct organizational loss in many disasters. For example, cold weather can destroy crops, or wild fires could destroy timber being collected and stored. As is the case with physical damage to assets, businesses can calculate precisely the damage done by disasters to raw materials.



### 3. Supply Chain Disruptions

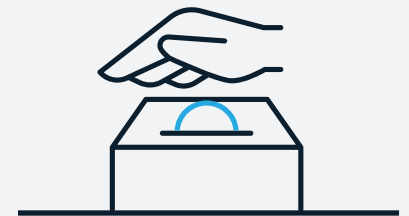
Unlike the previous two loss categories, supply chain disruptions are indirect organizational losses that may be a bit more difficult to calculate. The more corporations rely on supply chains, the greater the effect of a disruption.

For example, if a manufacturer relies on shipments of raw materials, production could be severely delayed if a main road gets washed out due to a flood. In turn, this could lead to delayed shipments of finished goods to retailers, which may even affect contractual obligations. Of course, if supply chains aren't so tightly run and aren't as important, then the damage may not be as severe.

### 4. Workers are Unable to Do Their Job

This is another indirect organizational loss. During severe weather events, people may not be able to attend work or even if they can, they may not be able to operate at peak efficiency. Power outages, Internet outages, inability to use the appropriate tools and other similar issues may cause downtime, which can lead to significant losses.

Natural disasters cause a lot of issues for businesses, in both direct and indirect losses. Consider all the different impacts of natural disasters, ranging from lost sales and income to regulatory fines. From there, steps such as uninterruptible power supplies to better site selection can be taken to mitigate – if not outright prevent – many of the dangers associated with weather-related threats.



### Every \$1 spent

on disaster preparedness can prevent \$7 worth of disaster-related economic losses, according to the University of Boston.

## How to Prepare for Natural Disasters

Once you've identified the greatest risks that a natural disaster presents to your organization, the next step is to create step-by-step business continuity plans for the critical business functions of the organization.

### 1. Identify critical business functions.

This is an exhaustive task but critical in preparing for a disaster or disruption. Critical business functions are activities that are vital to your organization's survival. Typically, critical functions are: 1) highly sensitive to downtime, 2) fulfill legal or financial obligations to maintain cash flow, 3) play a key role in maintaining the business' market share or reputation, and/or 4) safeguard an irreplaceable asset. For many organizations today, IT systems and networks are a top priority to get back up and running after a disaster.

### 2. Create business continuity or emergency action plans.

You need to have detailed documentation that clearly outlines roles, responsibilities and action plans for each of the critical business functions. These plans should include up-to-date contact information, emergency contacts, a clear chain of command, evacuation and contingency procedures, and step-by-step instructions to ensure the safety of employees and recovery of critical business functions.

### 3. Communicate.

While there is no question that communication is critical during a crisis, communicating with your organization outside of a crisis is equally important. Often, the only time employees or stakeholders ever hear from the crisis or continuity teams is during a disaster. This should not be the case, and you need to develop regular communications with employees as part of your program. They should know what to expect and have a good understanding of the recovery plan well before the event occurs.



---

One company even hired a marketing agency to help communicate their continuity and crisis program to employees.

While not everyone can afford to do this, the concept of communication is quite simple; get out of your box and spread the word!

#### 4. Test the plans... and then test them again.

We can't tell you enough how important it is to test your plans regularly and consistently. Many companies use an HR system to track employee information, but surprisingly, these systems don't validate phone numbers. Imagine the mess you'd have on your hands during a crisis if something as basic as employee contact information was inaccurate or outdated. It's great to have an emergency preparedness plan, but it won't be particularly helpful if it falls apart once executed.

#### 5. Don't become complacent.

It doesn't matter where businesses are located, natural disasters can happen anywhere, at any time. Just because your company hasn't experienced an earthquake in 20 years, that doesn't mean it couldn't happen tomorrow. Unprepared companies are the ones that suffer the greatest losses, so risk managers need to ensure they don't become complacent when planning for these events. Conduct training that details a variety of emergency responses, from a cardiac arrest incident or fire, to a natural disaster such as a tornado or earthquake. Taking a proactive approach will help employees react without panic if a large-scale emergency were to occur.



#### Try a tabletop exercise

or a simulation to test the effectiveness of your plans.



## 3 Steps to Better Disaster Recovery

The event that you've dedicated your entire career preparing for has arrived. Whether it's a natural disaster, power failure, cyberattack, or even a corporate scandal, your disaster recovery plans are locked and loaded.

Disaster recovery is never a simple task, so follow these three best practices to ensure your recovery efforts don't get stymied.

### 1. Leverage technology

There are many technology solutions for disaster recovery. Customize what you're working with, or consider a tool specifically for disaster recovery. Depending on your budget and how sophisticated your BC/DR program is, technology solutions can send emergency notifications, activate runbooks, facilitate exercises, risk assessments, incident management, business impact analyses and even manage your entire disaster recovery program from start to finish.

### 2. Ensure everything is documented

Insurance can be a truly effective risk management tool to help enterprises bounce back after a catastrophic event. However, insurance providers are likely to look for ways to get out of claims or reduce them. Firms need to be able to prove their claims, and that requires accurate documentation and evidence of what occurred and what is covered by policies.

Documentation plays a critical role in effective disaster recovery, and dealing with insurers is only one of the benefits. This paperwork can grant risk managers greater insight into how the company was taken by surprise by natural disasters and improve business resilience and monitoring efforts in the future. This enables firms to be more proactive and helps preserve company value more effectively in the long run.

Be sure to  
understand your  
insurance policy and  
what is covered!

U.K.-based videogame developer Hello Games lost everything in 2014 after a nearby river flooded. To make matters worse, insurance didn't cover the incident because the firm was located in a flood zone.



### 3. Communicate across departments

We mentioned communicating with your staff prior to and during a crisis, but the aftermath of a disaster is an especially important time frame. Internal conversations are critical to ensuring recovery efforts are executed without a hitch. Failure to coordinate effectively may hinder recovery, and it could also leave people with an incomplete picture of what happened and why.

This should be extended to interactions with third parties associated with the recovery process as well. Whether it's insurance agents or repairmen, open communication makes everyone's job easier and reduces wasted recovery efforts.



## Lessons Learned from Hurricanes Harvey & Irma

Organizations without an adequate emergency preparedness plan learned a hard lesson in late August and September of 2017. Hurricane season of 2017 showed its might, and while most businesses will never experience a single hurricane in their lifetime, some dealt with four hurricanes in almost as many weeks. Hurricanes Harvey, Irma, Maria and Nate wreaked havoc and were some of the strongest storms in recent history that caused significant damage and widespread devastation across the United States and Central America.

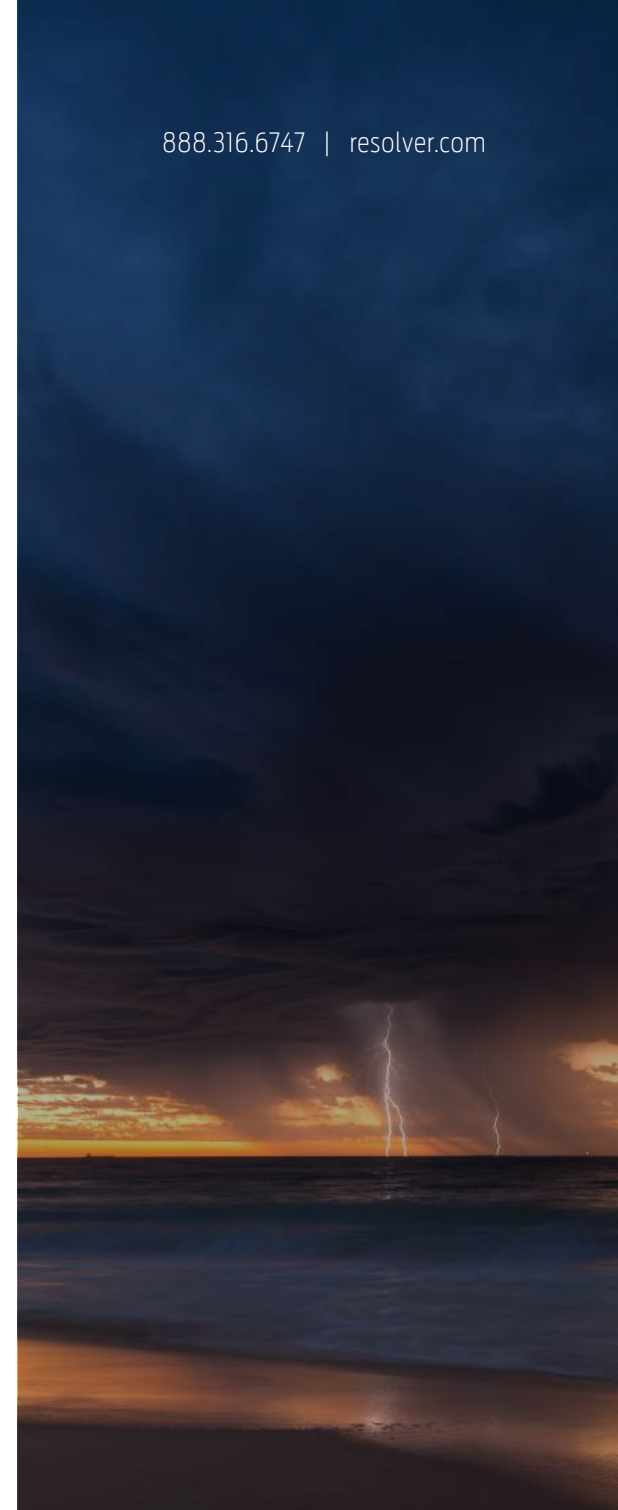
Here's what your organization can learn from the hurricane season of 2017:

### 1. This is real life.

Recognize that events like this will happen. Many businesses affected didn't anticipate back-to-back disasters and didn't have staff rotations accounted for in their emergency response plans. Just remember, the event that will have the most devastating impact on your business is also the one you never thought would happen. We live in a crazy time – devastating storms, terrorism, mass shootings... don't play the numbers game. Be a realist and be prepared. It is your responsibility after all.

### 2. Disasters have a domino effect.

While back-to-back devastations are rare, a single disaster can have a domino effect. During a disaster, emergency response teams are spread thin and when resources are solely focused on the big event, other smaller events will occur and it's almost always something you didn't think of during planning. It could be an internal event or even a government decision, a Facebook post, a crisis at a related company. The key is to prepare for a cluster of crises to occur, because they will.



### 3. Executives are leaders but in an emergency, they need to follow.

At almost any business resilience conference there are sessions on “how to get executive buy in for planning”. While no one is questioning the importance of executive buy in, it can be even more important to know how to manage executives during a crisis. Why do they need to be managed? Well, executives are used to taking the lead and making the decisions. But let’s be honest, execs are rarely involved in BC/DR planning. You build plans. You assign resources. You exercise. And then the event occurs and the company’s reputation, customers, revenues are on the line... and guess who steps in? Executives do what they do best, which is to manage, make decisions and direct, but their involvement often causes confusion and disruptions during a crisis response. Be sure your plans clearly define who is making decisions during a crisis.

### 4. Out of sight, out of mind?

Puerto Rico is a territory of the United States, and while it’s not a U.S. state, residents of Puerto Rico are natural born American citizens just like those in the U.S. – apart from voting rights in Congress or the Electoral College. Despite this, recovery efforts in Puerto Rico have been minimal compared to the response to Harvey and Irma. Was Puerto Rico simply too “out of sight, out of mind”? Or perhaps emergency response teams were too tired by the time the third hurricane hit? For businesses with locations outside of the United States, you must include these regions in your BC/DR plans. And don’t forget to test them. The devil is in the details which can vary by geography and many other factors.



Did you know that Puerto Rico SMS text traffic is different than in the U.S. and Canada?

The same short codes that work in the U.S. and Canada don’t work within Puerto Rico. There are even variances between mobile network carriers in Puerto Rico.

## Achieve True Business Resilience with Resolver

At Resolver, we understand that business resilience comes with its unique challenges – that's why over 1000 of the world's largest companies trust us to protect what matters.

Resolver's approach to business resilience is simple: Business continuity, disaster recovery and emergency notifications all fall under business resilience, which is why our platform does it all. Easily manage your entire program and use the many automated features to streamline processes, activate plans, send notifications and ensure compliance. Visualize your entire program, identify gaps in your planning and bring it all together in a single, integrated view.

Reach your full potential with Resolver. Prevent loss. Recover faster. Make better decisions.

In today's world, there is only one thing for certain: uncertainty.

Prepare for the unexpected with Resolver and achieve true business resiliency.

