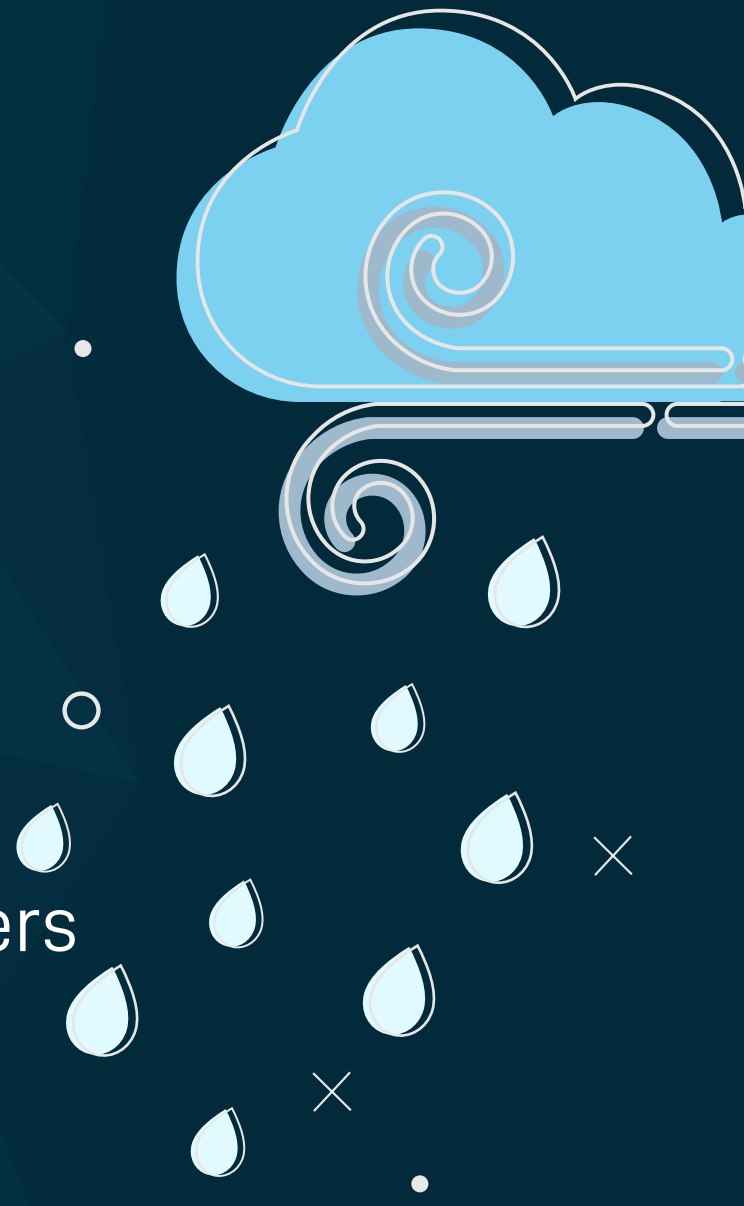
EBOOK

datto



Natural Disaster Survival Guide for Businesses

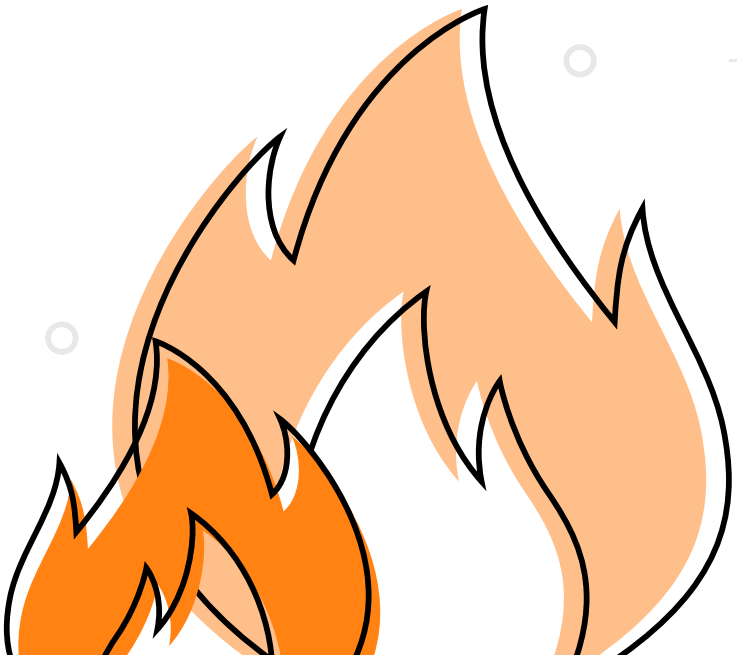
A Quick Reference for Business Leaders

Every business has to prepare for the worst. Those that don't may never fully recover from a disaster. But not all disasters are created equal. And not all businesses are at risk for every kind of disaster. That's why Datto put together this quick Disaster Survival reference guide to help you ensure that your business can keep operating even if it's struck by one of the natural disasters described.

Of course, this eBook is no substitute for rigorous business continuity (BC) planning with a certified BC consultant. But it will get you started in the right direction—and help ensure that you have the basics of a good disaster recovery in place even before you invest in a more formal BC plan.

Note: This guide addresses continuity of business operations only. It does not address the physical safety of employees during a disaster—which should always be the first priority. For matters of employee safety, please consult appropriate guidance from building codes, fire safety engineers, etc.

A large fire, of course, can force a business to have to **relocate all of its operations** temporarily or permanently.



Disaster #1

BUILDING FIRE OR FLOODING

Description:

Fires or floods within an office or building can range from small incidents of short duration to the complete destruction of the facility.

Potential impact:

Even a relatively small fire/flooding incident can have a very disruptive impact on a business. For example, a small fire in an office on an upper floor can result in the complete flooding of computers and telephone systems in the offices below as the building's sprinkler systems kick in and firefighters seek to extinguish the blaze.

Similarly, even a relatively limited amount of water leaking from a broken pipe or valve can put some or all of a business's technology infrastructure out of commission.

A large fire, of course, can force a business to have to relocate all of its operations temporarily or permanently.

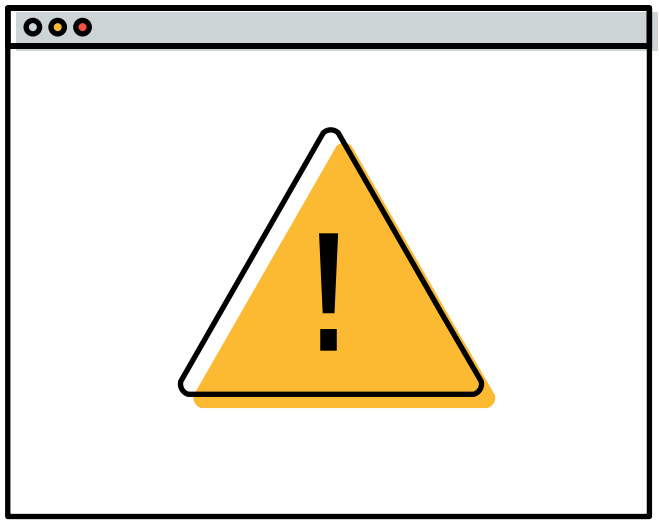
Risk factors:

There are approximately 100,000 commercial building fires in the U.S. per year, according to the National Fire Protection Association. Those at highest risk include manufacturing facilities, as well as offices located above or in proximity to restaurants because cooking is a primary cause of non-residential structure fires, just as it is in homes.

Warning times:

Water damage from failed plumbing, sprinkler systems, etc. can short-circuit electronic equipment with zero warning. However, building alarm systems

Prepare an emergency posting for the company website **that can be activated immediately and progressively** as the consequences of the event unfold.



typically give employees a few minutes to shut down critical systems and evacuate the premises.

Technology continuity:

As noted above, the severity and length of business disruptions caused by fires and flooding can vary considerably. To be prepared for extended or permanent facility damage, businesses should:

Maintain continuous off-site backup of data, applications, and server images.

Have arrangements in place for re-routing incoming calls to an alternative site and/or to employees' mobile phones.

Prepare an emergency posting for the company website that can be activated immediately and progressively as the consequences of the event unfold.

People continuity:

Because building fires and flooding only affect individual structures (or, at worst, just a few adjoining ones as well), businesses impacted have a lot of options for keeping people productive. Business Continuity plans should include:

Arrangements in advance with a nearby shared/furnished office space provider, hotel, college, or other facility for an immediate/temporary operations command center.

Next-day workspace provisioning in another company facility, emergency failover "cold site," or at home personal desktops/laptops with appropriate call forwarding.

Internal communications for keeping employees updated on resource availability, recovery status, etc.

Any necessary third-party contracting for shipping/receiving, mail processing, duplicating, etc.

Businesses may also seek policy provisions that address work done from home or other locations while the facility is under repair (and/or a new location is secured) as well as business losses that may occur despite best–effort BC planning and execution.

Process continuity:

Again, because building fires and flooding are highly localized, they typically only disrupt processes that touch a single company location. Business continuity plans therefore need to provide for alternative locations and means to perform actions such as:

- Answering phones
- Processing orders
- Issuing invoices
- Signing checks
- Filing reports required by regulatory mandates

Insurance considerations:

A properly insured business should have a policy that covers the expenses above, in addition to the physical damage directly caused by the fire or flood. Businesses may also seek policy provisions that address work done from home or other locations while the facility is under repair (and/or a new location is secured) as well as business losses that may occur despite best-effort BC planning and execution.

Disaster #2

HURRICANE OR COASTAL STORM

Description:

Hurricanes and coastal storms wreak destruction through a combination of high winds and heavy rain. They may also be accompanied by surging tides that flood that affected area with salt water.

In the event of a regional disaster, in addition to making sure their own operations continue uninterrupted, **businesses should be prepared to help their nearby customers and partners** get through the crisis.

Potential impact:

Hurricanes and coastal storms impact business in three primary ways:

Direct damage to operating facility due to high winds, flooding, and objects such as tree limbs and debris that become high-speed projectiles capable of smashing through windows, roofs and other structural elements.

Extended power outages, road closures, and other lasting damages can put a business facility out of commission for a week or more.

Regional impact can affect customers, suppliers, and business partners—as well as the homes of employees.

Risk factors:

About a dozen named storms occur along the Gulf and Atlantic coasts each year. Major disasters, such as Hurricane Katrina and Superstorm Sandy, underscore the potential damage that can result when such events strike population centers. Climate change may be increasing both the frequency and intensity of these events.

Warning times:

Businesses usually have significant advance warning of an approaching storm. However, because storm paths are notoriously difficult to predict, these warnings can often be false alarms. Some businesses therefore fail to respond to storm warnings due to the "Cry Wolf" syndrome.

Technology continuity:

Hurricanes and coastal storms can put a data center out of commission for a day, a week, or permanently. All businesses, especially those operating in storm or hurricane-prone areas, should be prepared for anything. Preparation should thus include:

The ability to restore IT operations in the cloud and/or at a site sufficiently further inland from the coast to be unaffected by the storm.

- Continuous off-site backup of data, applications, and server images.
- The ability to restore IT operations in the cloud and/or at a site sufficiently further inland from the coast to be unaffected by the storm. This restoration may require evacuation of key IT personnel out of the storm so that they can continue to work remotely from their laptops even if the area's mobile data services are interrupted.
- Website posting that alerts customers and partners about storm preparations—along with frequent post-storm updates that allows visitor to track the progress of any necessary recovery.

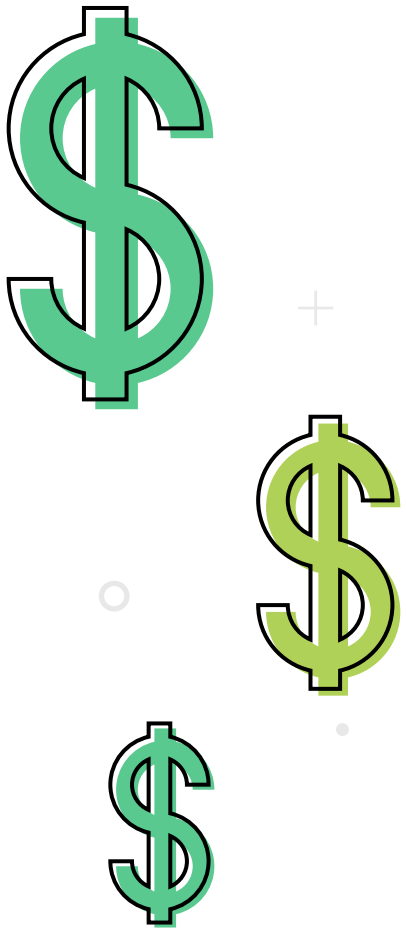
People continuity:

Major storms can affect entire regions for an extended period of time. Business continuity plans should include:

- Availability of a sufficiently distant inland facility—along with any temporary housing necessary for key employees whose homes are also in the path of the storm.
- Internal communications for keeping employees updated on resource availability, recovery status, etc.
- Any necessary third-party contracting for shipping/receiving, mail processing, duplicating, etc.

Process continuity:

In the event of a regional disaster, in addition to making sure their own operations continue uninterrupted, businesses should be prepared to help their nearby customers and partners get through the crisis. Planning should thus include:



- Communications in advance with local/regional customers and suppliers who may also be impacted by the storm. This communication should include alternative mobile contact numbers.
- Pre-determined policies regarding order turnaround times, invoice processing, scheduled service visits, and other activities likely to be affected by the storm.
- Direct servicing of customers by supply-chain partners, where appropriate and feasible.

Insurance considerations:

In the wake of a major weather event, businesses should ensure that their policy covers all aspects of business continuity, rather than just damage and outage impacts. Also, given the fact that businesses typically have significant advance warning of such an event, companies should avoid confusion by contacting insurers in advance to confirm exactly what steps both parties
will take in the storm's immediate aftermath.

Disaster #3

FLOOD

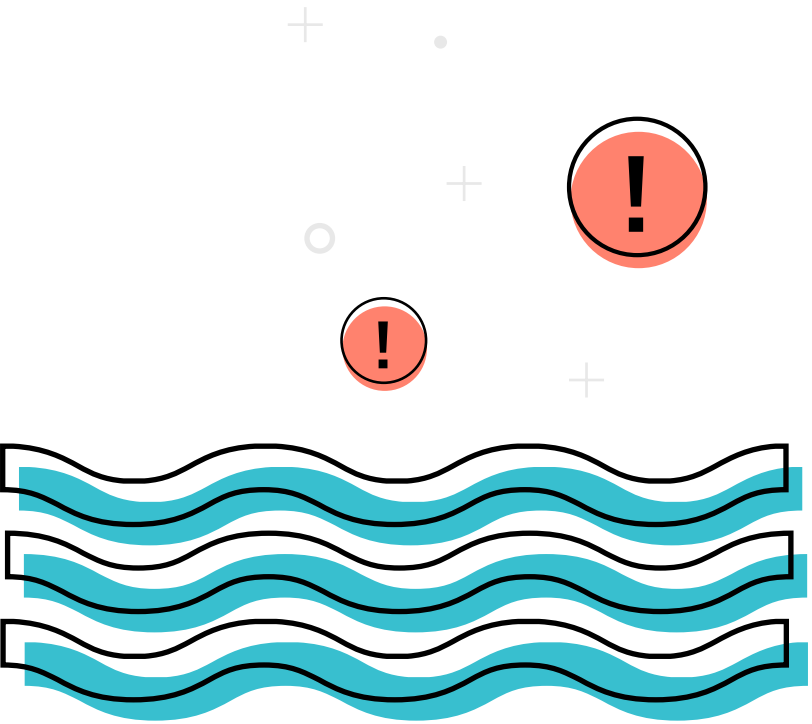
Description:

Floods typically result from excessive upstream precipitation and/or runoff. They can range from flash flood, which typically occur on smaller rivers, to slower rising floods across large low-lying areas.

Potential impact:

Floods can have their greatest catastrophic impact on business facilities located in basements and first floors. Floods can also significantly interrupt business functions

Businesses with any computer equipment located in basements or on ground floors **should take special precautions to protect their investments** by getting them up and off the floor, if possible.



through power outages, loss of communications, and road flooding that prevents employees from commuting to and from work.

Businesses should be especially cautious about asking employees, customers, or suppliers to drive when an area is under the threat of a flood since this is a leading cause of personal harm.

Risk factors:

According to the NOAA, damage due to flooding in the U.S. amounts to an average of almost $8 billion annually. Flood risk varies considerably by both probability and likely severity. The FEMA Flood Map Service Center (MSC) is the official public source for flood hazard information produced in support of the National Flood Insurance Program (NFIP).

Warning times:

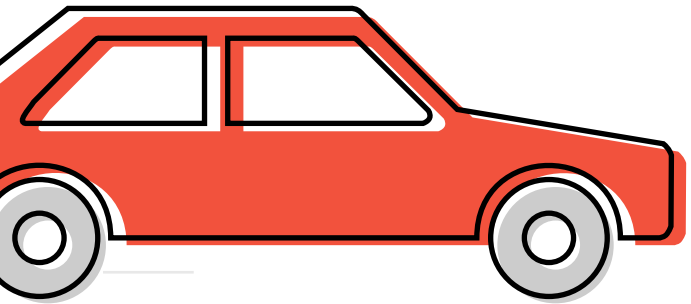
The National Weather Service and other agencies typically issue three types of alerts: flood advisory, flood watch, and flood warning. Advisory and watch alerts can give businesses 24 hours or more to prepare for an event.

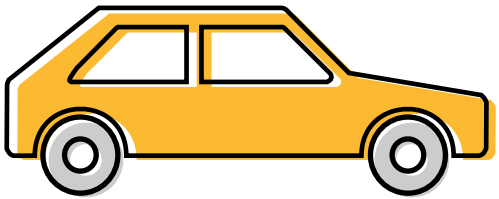
Technology continuity:

As noted above, businesses with any computer equipment located in basements or ground floors should take special precautions to protect their investments by getting them up and off the floor, if possible. Other appropriate precautions include:

- Increasing the frequency of off-site backups for data, applications, and server images.
- Preparation of an alternative worksite — including any necessary network/Internet connectivity, desktops/laptops, printers, routing of incoming calls, etc.

Under no conditions should employees be encouraged to commute through a flood–prone area.





- Emergency posting for the company website, along with timely updates as the extent and impact of the flood unfold.

People continuity:

Assuming an alert has been issued, businesses should not have employees report to work. Instead, arrangements should be made to have employees work from home, from the home of a friend or relative (if their home is within the projected flood area), or from an alternative facility well beyond the potential reach of flooding. If for some reason employees are on-site when a warning is issued, the facility should be quickly evacuated. Information about suggested evacuation route(s) should be shared with employees. Again, under no conditions should employees be encouraged to commute through a flood-prone area.

Process continuity:

Because floods can have extensive regional impact lasting for several days, businesses may need to make alternative provisions for customers and supply-chain partners:

- For customers within the flood area, businesses should obtain necessary information about their own flood preparations. This may include alternative worksites, key contacts' mobile phone numbers, etc.
- For customers not within the flood area, businesses should pro-actively communicate about the potential for a disruption and the steps being taken to avoid that disruption. Alternative plans should be made in the event that the business is still interrupted — such as direct servicing of customers by supply-chain partners, where appropriate.

- For supply-chain partners, plans should be made for emergency situations such as power outages and road closures. For example, decisions can be made not to ship goods to the business facility in order to avoid potential damage to inventory.

Insurance considerations:

Flood insurance is a highly specialized category within the broader property and casualty (P&C) market. Business owners should review their policies carefully to make sure they are covered for all potential types of loss at a fair price. In some cases, it may be necessary to obtain a flood policy from a separate underwriter specializing in flood-related business coverages.

Disaster #4

TORNADO OR EXTREME STORM

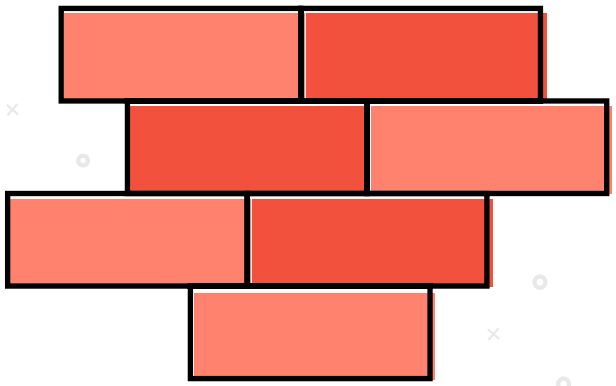
Description:

Tornados are extreme weather events characterized by funnels of wind that can exceed 100 MPH. They usually travel no more than a few miles before dissipating and are about 250 feet in diameter. They can, however, be much wider and travel much further. Under the right conditions, multiple tornadoes can form in a single given region. The same storm cells that cause tornados can also bring intense hail and/or lightning.

Potential impact:

Tornados are extremely destructive in a relatively narrow swath. They also tend to pass quickly. So while the structure in which a business is located can suffer intense damage — or even complete destruction — broader regional infrastructure for transportation and communications usually remains functional.

The best shelter is usually in an interior room in the lowest possible floor—**away from doors, windows, corners, debris**, etc. Make sure all employees know where this shelter is.



Risk factors:

About 1,000 tornadoes form in the U.S. every year — although many of those do so without threatening property or people. The vast majority of tornadoes occur in the Great Plains colloquially known as "Tornado Alley." However, tornadoes and extreme storms can occur in other parts of the country as well.

Warning times:

The National Weather Service issues tornado watches and warnings. Warnings are issued when a tornado is spotted or indicated by radar and, on average, provides around 15 minutes advance notice of impact.

Technology continuity:

Any business in the path of a tornado will have to prepare for the complete destruction of their technology infrastructure. This means:

- Complete, fully up-to-date off-site backups for data, applications, and server images.
- On-demand availability of failover IT infrastructure in the cloud or at an alternative facility.
- On-demand availability of failover voice/fax call switching, such as a hosted PBX service.

As with other disaster, businesses in tornado-prone areas should also be prepared to use their website to continuously update customers about disaster impact and disaster recovery progress.

Commercial property insurance typically covers any structural damage by a tornado. Business interruption insurance, however, is necessary to cover both recovery costs and loss of earnings until operations can resume.

People continuity:

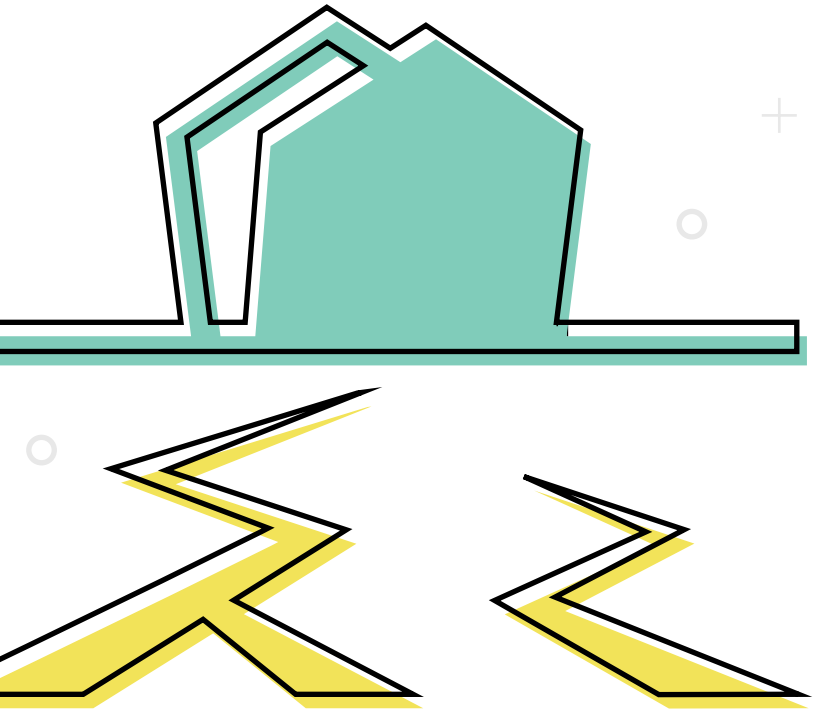
Businesses operating in areas susceptible to tornadoes should the following steps to ensure the safety of employees and other stakeholders (customers, suppliers) who may be on-premises when a tornado strikes:

- Designate a tornado shelter. The best shelter is usually in an interior room in the lowest possible floor — away from doors, windows, corners, debris, etc. Make sure all employees know where this shelter is.
- Prepare a tornado survival kit that includes food, water, flashlight, extra batteries, etc.
- If pre-tornado weather conditions exist before work or before a shift, have people work from home wherever practical.
- Assign one or two employees to continuously monitor weather alerts for as long as such conditions persist. Do not count on this "just happening."
- Ensure that all employees and site visitors know exactly where the closest shelter is and what the alert will be.
- Encourage any site visitor who might be planning to leave the site while tornado conditions persist to remain there until the present threat has passed.
- Have a system in place to track both who is in the building and who is in the designated shelter.

Process continuity:

Because tornadoes can have catastrophic impacts on physical facilities, businesses must plan ahead for an alternative way to carry out everyday processes

Earthquakes can affect businesses both directly (tremors that can injure people, damage facilities, cause equipment to fall and break, etc.) **and indirectly** (road damage, broken water mains and gas lines, resulting fires and floods, etc).



such as answering phones, processing orders, issuing invoices, signing checks, etc. Also, as with other types of disasters, businesses must pro-actively communicate with stakeholders the potential for a disruption and the steps being taken to avoid that disruption.

Unlike other types of disasters, a tornado can completely devastate businesses and homes on one block while leaving those on another completely unscathed. For this reason, businesses in tornado-prone areas may also want to consider what their planned role will be in helping affected customers, neighboring businesses, and the community in general to recover from a tornado even if they are not directly affected.

Insurance considerations:

Commercial property insurance typically covers any structural damage caused by a tornado. Business interruption insurance, however, is necessary to cover both recovery costs and loss of earnings until operations can resume. Companies should be wary of "anti-concurrent causation" clauses in their existing policies that can give insurers grounds to deny a claim if damage that occurred during a tornado can be attributed to an ancillary cause.

Disaster #5

EARTHQUAKE, LANDSLIDE OR AVALANCHE

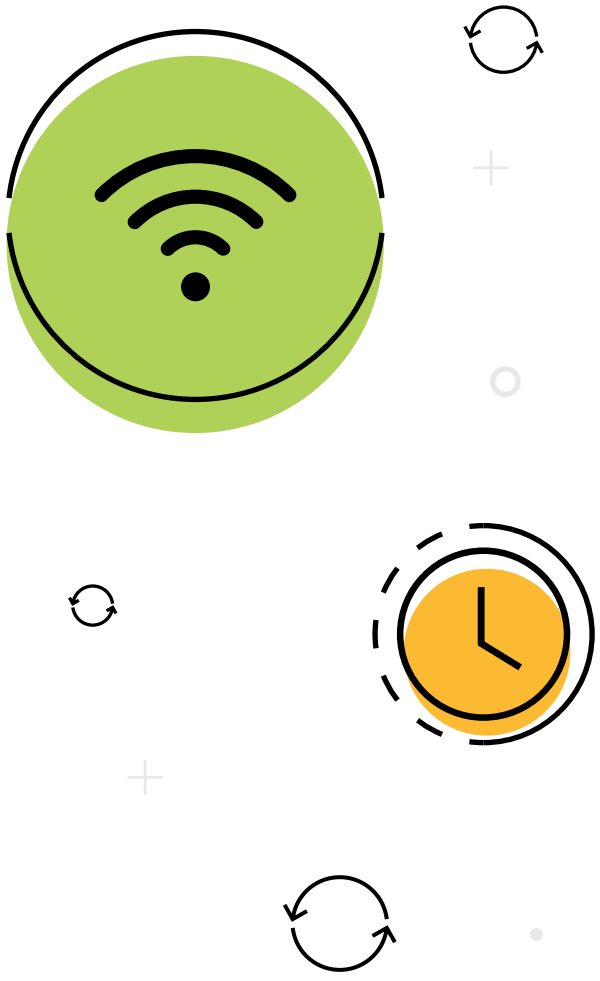
Description:

Seismic events and other disasters can result from the inherent instability of earth, rocks, snow, etc.

Potential impact:

Earthquakes can affect businesses both directly (tremors that can injure people, damage facilities, cause equipment to fall and break, etc.) and indirectly (road

Wireless network failover for maintaining a modicum of connectivity in case of a local fiber break.



damage, broken water mains and gas lines, resulting fires and floods, etc). Landslides and avalanches can take out roads and utilities and damage buildings.

Risk factors:

Earthquakes primarily threaten business in known areas of seismic activity, such as the West Coast and the New Madrid fault. Smaller tremors, however, can also impact businesses in many areas. Other earth-related hazards mainly threaten businesses located in mountainous regions.

Warning times:

Earthquake early warning systems are available, but may give only a few seconds advance notice of an event depending on the distance from the epicenter.
Some slow-moving mudslides, in stark contrast, may give businesses hours or even days to prepare.

Technology continuity:

Like all businesses, those in earthquake zones should maintain continuous off-site backup of data, applications, and server images. However, these businesses can take further precautions to avoid operational disruption in lighter tremors that do not require a complete failover. These precautions include:

- Use of data center racks and enclosures that can tolerate limited seismic activity and protect sensitive equipment from excessive shaking.
- Failover power supply to keep equipment running and/or allow time for orderly shutdown in the event of a power outage.
- Wireless network failover for maintaining a modicum of connectivity in case of a local fiber break.

People continuity:

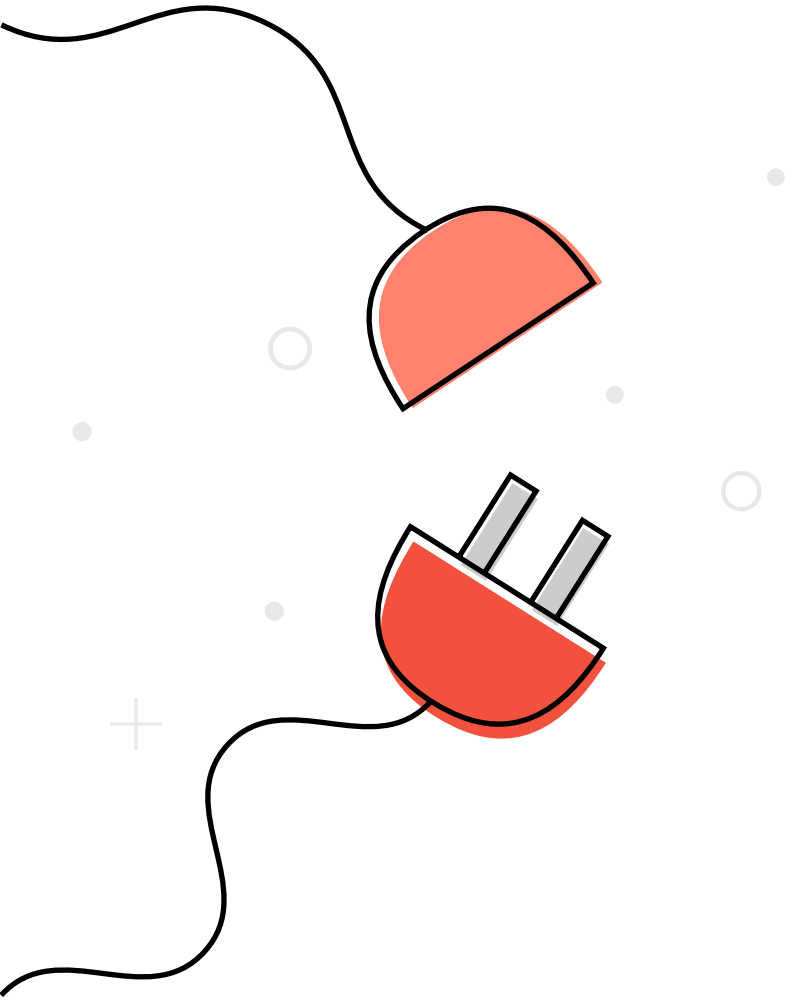
Businesses in earthquake-prone areas should ensure the safety of employees and other stakeholders (such as customers or suppliers) who may be on-premises when an event occurs. Appropriate measures include:

- Picking "safe places" in advance, such as under a sturdy desk or against an interior wall away from windows or tall, unstable office furnishings. Short distances are key, because statistics indicate that people moving as little as ten feet during a tremor are the most likely to be injured.
- Training employees in proper actions, such as waiting in their safe place until the shaking stops completely before attempting to help others, being prepared for aftershocks, using stairs instead of elevators, etc.
- Awareness of fire hazards and the location of fire extinguishers, as fire is a primary post-earthquake hazard.

Process continuity:

The regional/local impact of earthquakes can be extremely haphazard, with some buildings suffering severe damage while nearby ones escape serious consequences. To be prepared for a worst-case scenario, businesses should:

- Plan an alternative means of performing everyday processes from home, a failover facility sufficiently distant not to be affecting by local seismic activity, or some combination of the two.
- Perform a damage assessment using a predetermined checklist and initiate remediation procedures.



- Pro-actively communicate with customers and suppliers regarding the status of the business and the progress of recovery, as well as policies regarding orders, shipping, accounts, etc.

Insurance considerations:

Earthquake policies covering structural damage often have high deductibles, ranging from 2-20% of a building's value. Insurance companies also tend to subject insured properties to rigorous inspection — and may require significant structural upgrades, such as bolting and bracing.

Disaster #6

HUMAN ERROR AKA "HURRICANE HUMANITY"

People make mistakes. They pull the wrong plug, click on the wrong link, open the wrong email attachment, or completely botch a major systems upgrade. They trip, spill and sync unapproved third-party apps to the network. They visit unsafe websites. They accidentally or maliciously delete business critical files. It's only natural, we are humans.

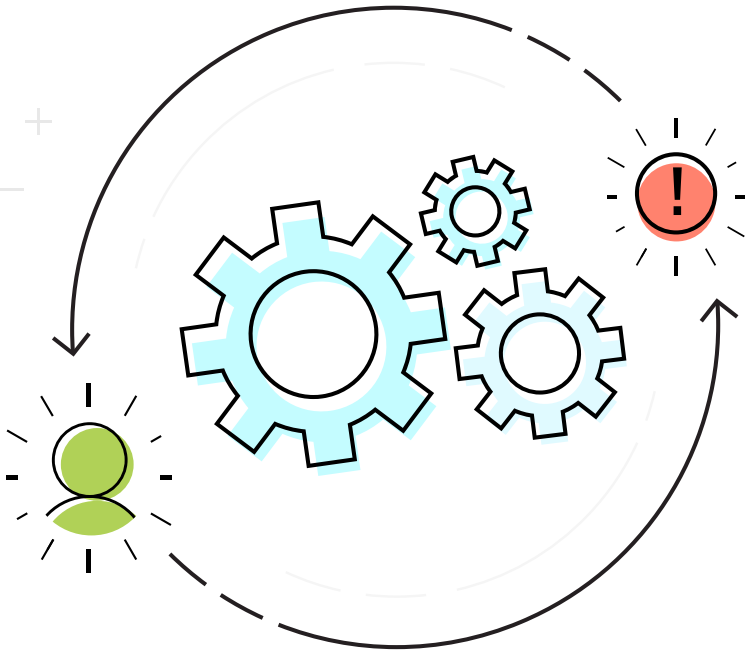
Potential impact:

Human error can cause your business to lose a single important file, account, server or completely shut down your critical systems.

Risk factors:

The Uptime Institute estimates that 70% of data center problems are caused by human error. Unless your business is entirely staffed by robots with fully redundant fail-safe error controls, you're at risk.

The Uptime Institute estimates that **70% of data center problems are caused by human error.** Unless your business is entirely staffed by robots with fully redundant fail–safe error controls, you're at risk.



Warning times:

No one will ever walk into your office and announce that today is the day they will make the biggest mistake of their lives, so don't expect any advance notice of human error (or any notice at all).

Technology continuity:

Have point-in-time backup that will let you quickly restore your data, application, and systems to the state they were in the moment before whatever happened happened.

People continuity:

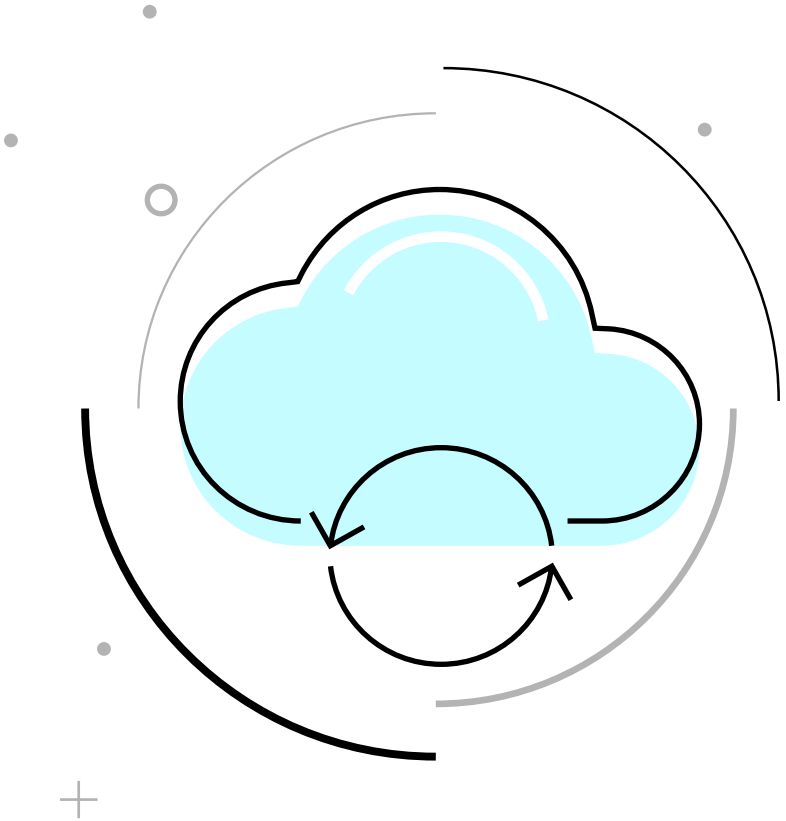
The potential for injuries and fatalities resulting from human error events are higher in certain industries, such as mining, aviation, and construction, however the consequences of human error can be just as undesirable in more sedate industries. Make sure your employees are trained on what to do during various "disaster" scenarios, whether it be a malware attack or someone accidentally deleting a critical directory. Make sure employees understand the situations that are high probability for the industry.

Process continuity:

The show must go on. So make sure you have the IT failover you need to make sure that it does.

Insurance considerations:

It's just about impossible to find an insurance carrier willing to write a policy that specifically covers oopsies.



Data backup is not enough. **In the event of a disaster, it's essential to be able to run applications on–demand from virtual machines** backed up in the cloud.

7 ADDITIONAL KEY PRINCIPLES OF BUSINESS CONTINUITY

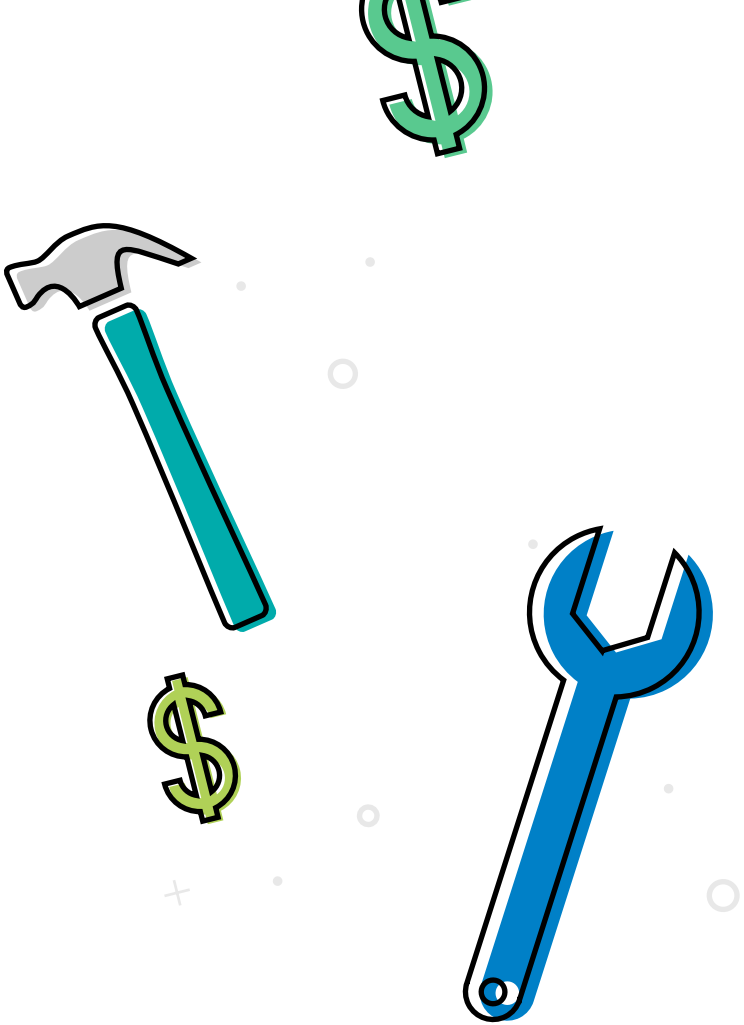
1. **Get employees involved.** BC plans only work if everyone understands them. Employees are also a great source of ideas and insights about how your business might be affected by a disaster. So business must communicate BC plans to employees regularly — and actively solicit their input.

2. Keep customers in the loop. Customers are the lifeblood of every business. They should be treated as such even during a disaster. Alerts on the company website, email broadcasts, social media and text messages to key contacts' mobile phones are all good ways for a business to express concern about the impact of a disaster on its customers. That level of service can even help transform a disaster into an opportunity for greater long-term customer loyalty.

3. **Collaborate with suppliers.** Businesses increasingly work in tightly interdependent networks of suppliers and partners. By working collaboratively with these third parties, businesses can make themselves even more resilient and well-protected against disasters large and small.

4. **Periodically test and update BC plans**. It's not enough to formulate a plan once and put it on paper. Assumptions about a plan should be validated with real-life testing. Plans also have to be updated continuously to ensure that they accommodate changes in the business's products, services, relationships, size, geographic reach, etc.

5. **Factor in compliance**. Businesses are subject to a variety of regulatory mandates that may require certain disaster preparedness measures. OSHA may be particularly relevant in regards to workplace safety.



6. **Examine insurance options carefully**. Coverages vary greatly, and policy language can be confusing. Businesses have to exercise careful legal and financial diligence to ensure that their policies cover all aspects of disaster recovery and revenue loss, not just the repair of initial damage. In some cases, it may make sense to obtain contingent business interruption insurance. This type of policy provides additional coverage for the harm a disaster can do to a business indirectly, for example, if a supplier in a different climate fails to deliver promised goods because of a local blizzard.

7. **Data backup is not enough**. Many businesses think they're safe just because they've backed up their critical files. The problem is that those files depend on applications and systems to be of any use to the business. That's why, in the event of a disaster, it's essential to be able to run applications on-demand from virtual machines backed up in the cloud.