Insurance Institute for Business & Home Safety®

staylocal™
building community awareness

WATER WORKS

READY FOR ANYTHING BUSINESS RESILIENCY WORKSHOP

June 30 - July 2, 2015

I. IBHS Intro presentation (~45 minutes)

II. Business Preparedness in New Orleans: A Snapshot (~3 minutes)

III. Shocks + Stresses Exercise (~15 minutes)

IV. Case Studies (~45 minutes)

IV. Wrap-up (~15 minutes)

- Lessons learned, future opportunities to engage
- Re-entry sign-ups
- Participant surveys completed
- Door prize raffle

Insurance Institute for Business & Home Safety®

staylocal™ building community awareness

WATER WORKS

Business Preparedness: A New Orleans Snapshot

Businesses along four commercial corridors were surveyed in early June 2015 by Metro NOLA SourceLink as part of the City of New Orleans' Disaster Resiliency Plan. They were asked several questions, including the following:

1. **Do you have a written emergency plan for your business?**
   - ***53% have no written emergency plan.***

2. **Do you have a communications plan for contacting your employees and customers in the event of an emergency?**
   - ***39% have no communications plan.***

3. **Do you have a written business continuity plan to ensure your business is prepared to overcome a range of disruptions to normal operations?**
   - ***66% have no written continuity plan.***

4. **Do you have backup generators?**
   - ***57% do not have backup generators.***

5. **Do you have flood insurance?**
   - ***20% do not have flood insurance.***

6. **Do you have business interruption insurance?**
   - ***43% do not have business interruption insurance.***

7. **Does your business have any mutual aid agreements in place to work together with other businesses before and after an emergency and/or disaster?**
   - ***75% do not have any mutual aid agreements in place.***

NOLA READY **Are you ready?** **get informed. get prepared. get ready**

City of New Orleans: Coming Home & Re-Entry Placards

After a mandatory evacuation, New Orleanians can return when the City deems it safe for citizens. New Orleans uses a tiered plan for re-entering the city after a mandatory evacuation: tiered re-entry means citizens and business come back at different times, allowing all possible essential services that citizens would need, such as power, food supply, etc., to get back and up and running. Businesses must register for a re-entry placard to be assigned to a tier that re-enters before citizens. Businesses will receive a Tier level and a certain number of placards for the vehicles needed to re-enter the city.

The application process for a re-entry placard can be completed online once an account has been established. These placards allow businesses to re-enter the city earlier than residents in order to assess damages and begin their efforts towards re-opening.The application is brief and only asks for some basic information on the business.

The website is: http://reentry.nola.gov. *The tiers include:*

Tier-1 re-entry placards are issued to major utility companies, pre-designated government contractors, suppliers of emergency relief goods and equipment and others necessary for the restoration of critical infrastructure and the support of emergency response efforts.

Tier-2 re-entry placards are issued to businesses that are essential to the return of residents of the parish and/or for the restoration of the economy, and to pre-approved humanitarian relief agencies. Approved Tier-2 businesses will be provided with a limited number of re-entry placards for damage assessment and recovery teams. Examples of Tier-2 businesses are fuel distributors, food and grocery stores, pharmacies, insurance companies, health care providers, hardware and building supply stores, facilities with fragile inventories such as, chemical processing and storage, laboratories, etc., large retailers of household goods and construction industry trades (plumbing, roofing, etc.). PLEASE NOTE: Only designated company employees will be allowed re-entry during Tier-2, not including family members and non-employees.

Tier-3 re-entry placards will be provided to businesses that are necessary for the return of the Parish's residents and restoration of its economy. All employees of Tier-3 credentialed businesses will be allowed re-entry. PLEASE NOTE: The immediate family members of the employees of Tier-3 credentialed businesses may re-enter the Parish while traveling with the properly credentialed Tier-3 employee.

Questions can be directed to Carlos at NOHSEP: 504-658-8714

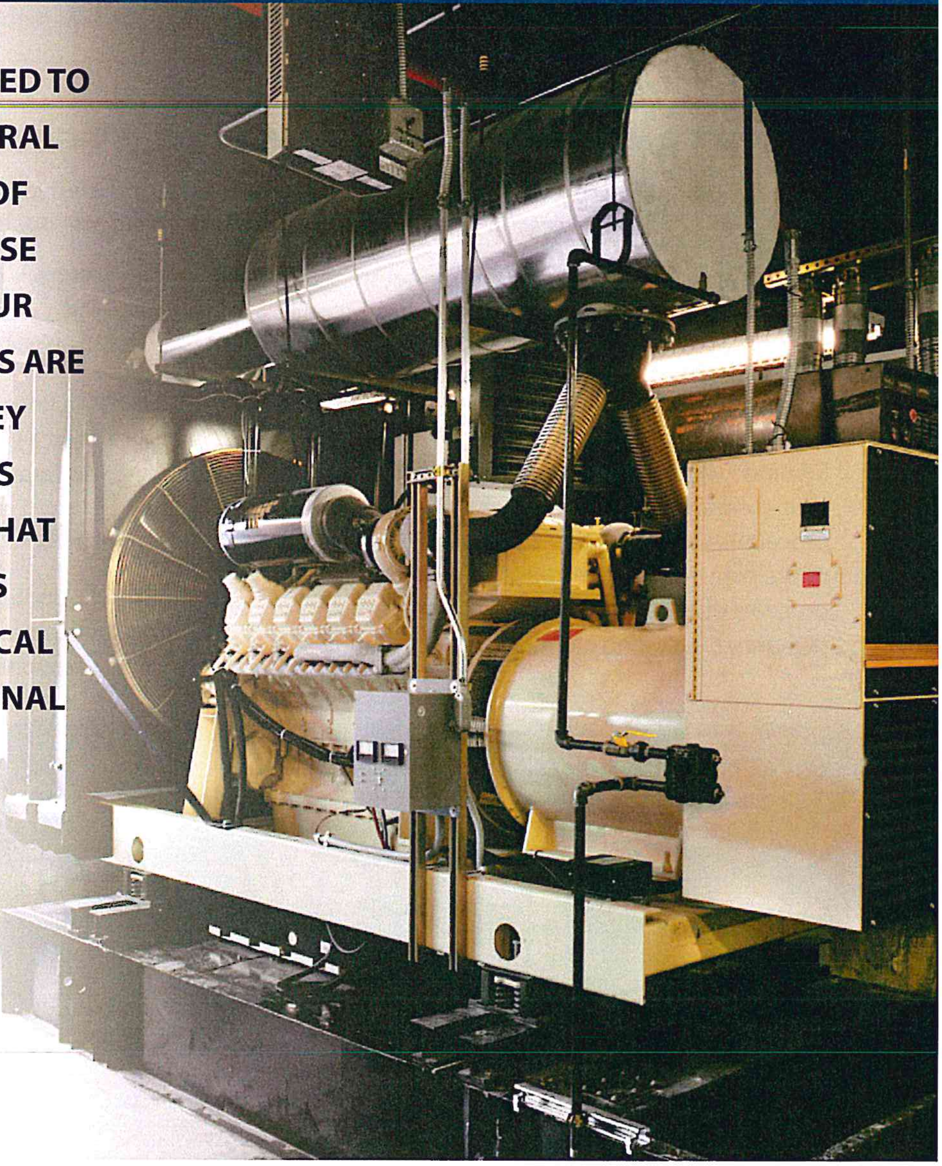
2013 COMMERCIAL SERIES

Insurance Institute for Business & Home Safety

How to Navigate Stormy Weather:

EMERGENCY PREPAREDNESS AND RESPONSE PLANNING

MANY BUSINESSES ARE NOT PREPARED TO RESPOND TO A MAN-MADE OR NATURAL DISASTER. STATISTICS SHOW THAT, OF THE BUSINESSES THAT CLOSE BECAUSE OF A DISASTER, AT LEAST ONE IN FOUR NEVER REOPENS. SMALL BUSINESSES ARE PARTICULARLY AT RISK BECAUSE THEY MAY HAVE ALL OF THEIR OPERATIONS CONCENTRATED IN ONE LOCATION THAT IS DAMAGED OR DESTROYED. THAT IS WHY DISASTER PLANNING IS A CRITICAL PART OF EVERY BUSINESS' OPERATIONAL OBJECTIVES.



To help keep small businesses "open for business," the Insurance Institute for Business & Home Safety (IBHS) has developed OFB-EZ (Open For Business-EZ), a streamlined business continuity program that gives business owners tools to better understand the risks they face; plan for how to contact key suppliers, vendors and employees; understand how to access data; and identify where to go for help after a disaster. Download the free OFB-EZ planning toolkit at: www.disastersafety.org/disastersafety/open-for-business-ez/.

OFB-EZ is an essential tool not only for business continuity but also to help identify priorities and organize essential information. Once this initial step is done, the next focus should be on emergency preparedness and response planning—the specific actions and tasks needed to protect people and property from physical and economic damage should disaster strike, as well as those to be taken directly following a disruption to your business. Not having a plan, or a having poorly prepared or misunderstood plan, could lead to disorganized preparation or confused response, with the possibility of harm to your employees or property.

Most storms and many other types of natural hazards can provide advanced notice and be tracked, which allows for at least some preparedness planning. But even if that is not the case, a number of the steps identified here will help to make your business more resilient and better able to withstand even an event that happens without warning.

COMPONENTS OF YOUR EMERGENCY PLANNING

Creating an emergency plan that deals with issues specific to your worksite and location is not difficult, time consuming, or expensive. The starting point should be your OFB-EZ (or other business continuity) plan, which identifies the risks to which you are most vulnerable. This will allow you to make sure that the emergency plan you create is right for the hazards or situations of greatest concern, such as severe weather, internal fire, chemical spills or other manmade disasters, civil disturbance, or building system failures.

The next step is to inventory your worksite layout, structural features, and emergency systems, so that you can tailor your plan to your situation. Just as with your business continuity plan, your emergency plan should include your employees in the planning process. While every employee eventually will be involved in how you prepare for and respond to an emergency, it makes sense to designate an Emergency Operations Team (EOT) to develop, oversee, and implement specific plans and procedures. The EOT should include a cross-section of employees, ranging from senior management to maintenance personnel, with all functional areas of your company represented.

GET A HEAD START IN ADVANCE OF SPECIFIC SEVERE WEATHER THREAT

While emergency planning ideally is a twelve-month priority, the start of the severe weather season in your area is a good time to refocus your efforts. This is the time to:

✓ Designate an employee to monitor weather reports and alert your team to the potential of severe weather.

✓ Review your business continuity plan and update as needed, including employee contact information.

✓ Remind employees of key elements of the plan, including post-event communications procedures and work/payroll procedures. Make sure all employees have a paper copy of the plan. Review emergency shutdown and start-up procedures, such as electrical systems, with appropriate personnel, including alternates.

✓ If back-up power such as a diesel generator is to be used, test your system and establish proper contracts with fuel suppliers for emergency fuel deliveries.

✓ Re-inspect and replenish emergency supplies inventory, since emergency supplies are often used during the offseason for non-emergency situations.

✓ Test all life safety equipment.

✓ Conduct training/simulation exercises for both your business continuity and emergency preparedness/response plans.

United States Natural Disaster and Severe Weather Seasons

While natural disasters and severe weather can strike at any time and in any location, there are specific times of year and geographic locations where certain types of disasters and severe weather are more prevalent. These are general guidelines, which vary depending on changes in annual weather patterns and other factors.

NATURAL DISASTER	SEASONS	GEOGRAPHIC LOCATION
Severe winter weather	Nov. 1 – Mar. 1	Northeast, Midwest, Mountain West, Northwest, High Elevations in Southwest
	Jan. 1 – Mar. 1	Mid-Atlantic
Flooding	Mar. 1 – June 30	Northeast, Mountain West, Northwest, Midwest
Flash Flooding	Year-round	Nationwide
Tornadoes	Mar. 1 – June 30	Midwest, Southeast, Southwest, Mid-Atlantic
Hurricanes	June 1 – Nov. 30	Gulf Coast & Atlantic Seaboard States
Thunderstorms and Lightning	Mar. 1 – Sept. 30	Central Plains, Southeast, Mid-Atlantic, Southwest
Hailstorms	Mar. 1 – Sept. 30	East of the Rockies
Wildfire	Mar. 1 – June 1	Southeast
	June 1 – Nov. 1	Mountain West, Pacific West, Southwest

LIFE SAFETY COMES FIRST

Every emergency plan should focus first on life safety protections:

✓ Procedures on how to report emergencies (fire alarm, dialing 911, calling an internal emergency number);

✓ Medical emergency procedures (who can perform them and to what extent, or will your business rely on the fire department or ambulatory services to provide these services?);

✓ Evacuation procedures (who can order an evacuation, under what conditions, how to evacuate, and what routes to take; etc.);

✓ Procedures on how to account for all employees after an emergency evacuation (sweep the area, check offices and restrooms, conduct roll call in the assembly area, etc.);

✓ Shelter-in-place procedures (who can order employees to shelter-in-place, actions employees should take before and while sheltering, etc.); and

✓ Shut down and start-up procedures including computer systems, special equipment, refrigeration systems if applicable, and building systems such as electric, gas and/or other utility systems.

5 DAYS BEFORE STORM CONDITIONS

START TO FOCUS ON WHAT NEEDS TO GET DONE

✓ Notify employees of the potential for severe weather and to be prepared for the emergency plan possibly to be implemented.

✓ Inspect the roof and grounds for loose debris, which may become a hazard in high winds. If staff or temporary help is available, begin removal of the debris, otherwise the removal may be done at the 72-hour interval.

✓ Provide a list of storm tips and needed supplies to help your employees prepare their homes and families. The Insurance Information Institute (III) has developed a free "Know Your Plan" app to help families make their own emergency plan; it also features property protection guidance from IBHS. The app is available in iTunes, or by searching "Insurance Information Institute" in the App store from any Apple device.

✓ Ensure all employees have your business' designated emergency telephone numbers and key contact other information (i.e., employee emergency wallet card).

72 HOURS BEFORE STORM CONDITIONS

TIME TO ACTIVATE THE PLAN

✓ If not completed already, remove or secure all loose roof and ground items, including landscaping that may become wind-borne debris.

✓ Clear roof drains, gutters and downspouts of debris, to prevent water back-up.

✓ Clean out all debris from outdoor perimeter drains, especially in areas where water may collect such as shipping and receiving areas where the ground slopes towards the building.

✓ Fill emergency generators with fuel and contact fuel suppliers with anticipated needs for post-storm deliveries.

✓ Ensure fire protection systems are in proper working order.

✓ Notify key customers, suppliers, and partners of office/facility closing and contingency plans (post office, Fed Ex, UPS, cleaning service, building management, vendors, etc.).

✓ Make decisions on when to excuse employees so that they have sufficient time to prepare their homes and families, and notify employees of office closure details.

✓ Make any necessary alternative travel arrangements for employees away on business.

✓ Customize messages for business' website, telephone recording, employee intranet, etc.

✓ Decide which outstanding invoices, bills, expense reports, etc. should be paid by your accounts payable department, before a possible closure.

✓ Instruct employees with laptops to take them home at the end of each day and confirm that they can connect to your business' server from home.

✓ Remind employees to make sure their cell phones are fully charged and that they have a power cord and car charger.

✓ Advise employees to begin checking your employee emergency hotline and/or company intranet/website for updates on the status of your office/facility.

48 – 24 HOURS BEFORE STORM CONDITIONS

FINALIZE PREPARATIONS AND MAKE SURE EMPLOYEES ARE SAFE

✓ Process accounts payable and payroll. Protect or relocate vital records.

✓ Make sure all employees with calling responsibilities have the most updated version of the company telephone call list and have it in multiple formats (hard copy, electronically, etc.).

✓ For hurricanes and other high wind events, install window protection; if window protection is unavailable, close all window blinds, and cover office equipment with plastic sheets or tarps.

✓ Close and lock all office doors, especially perimeter offices.

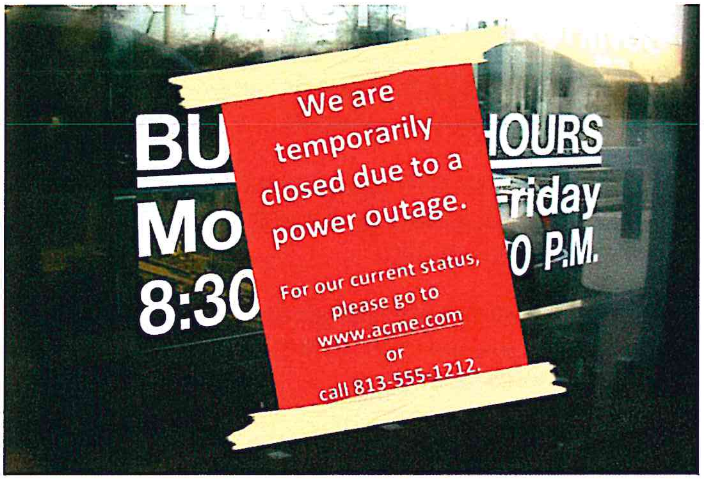
✓ If you expect your building to be exposed to flooding or storm surge, seal all water entry points such as utility penetrations into the building and install flood protection including first-floor drain plugs.

✓ Conduct full/partial shutdown procedures. If volunteers are to remain onsite during the storm, make sure they can remain in a safe and secure area. If conditions permit, instruct them on how to monitor, document, and mitigate against leaks and water infiltration in critical areas with vital equipment.

✓ Advise employees to check the status of your office/facility at least twice per day.

✓ Disconnect all electrical equipment and unplug from power source.

✓ Place a "Closed" notice on office/facility main entrance.



We are temporarily closed due to a power outage.

For our current status, please go to www.acme.com or call 813-555-1212.

Don't forget to post a notice on your front door if you close.

DURING AND IMMEDIATELY AFTER THE STORM

✓ Update employee emergency hotline and/or company intranet and company website with postings on the status of your operations.

✓ Activate the company telephone call list process, in order to contact all employees regarding the status of your office/facility.

✓ Designate times for key staff members to call into conference calls for situation overviews.

RECOVERY: AFTER THE STORM

✓ Designated personnel should return to the facility, assess conditions, document damages, and notify the emergency operations teams of their findings.

✓ When it is deemed safe, designated personnel should begin start-up procedures.

✓ When all safety and operational concerns are addressed and an "All Clear" is provided, employees can return to work.

✓ Activate employee communications tools and local media contacts to give notice of re-opening.

✓ Take an overall inventory, including photos of all damaged property, and report damage and related expenses to your insurance company.

✓ Employees returning to the building should be instructed to examine their work area, test all office equipment and report findings back to the designated staff contact.

✓ Notify key customers, suppliers, and partners of office/facility re-opening and any necessary property or operational changes resulting from storm damage.

Inspect and inventory any damage to your property.

LONGER-TERM PLANNING AND REPAIRS

Once you get through a major disruption, it is important to remember that the next storm season is only a few months away. Now is the time to begin inspecting your building and premises and initiating repairs to the building envelope (roof, windows, walls, doors), as well as improvements that will help you to reduce damage in the future. IBHS provides a wealth of resources on strengthening your buildings against natural hazards on its website at: www.disastersafety.org/commercial_maintenance/.

This is also the time to debrief on the successes and shortcomings of your emergency plan, compile a log of actions to be taken, and incorporate improvements into your plan for the future. You also should make sure that you are ready should another disaster occur without warning by replenishing your disaster/emergency supply kit, and updating your plan every time you have a significant change in operations, equipment, or employees. Finally, remember that your team's ability to safeguard themselves and your business in an emergency reflects their understanding of the overall plan and their own responsibilities, so practice during the off-season so that everyone is prepared on game day.

2014 COMMERCIAL SERIES

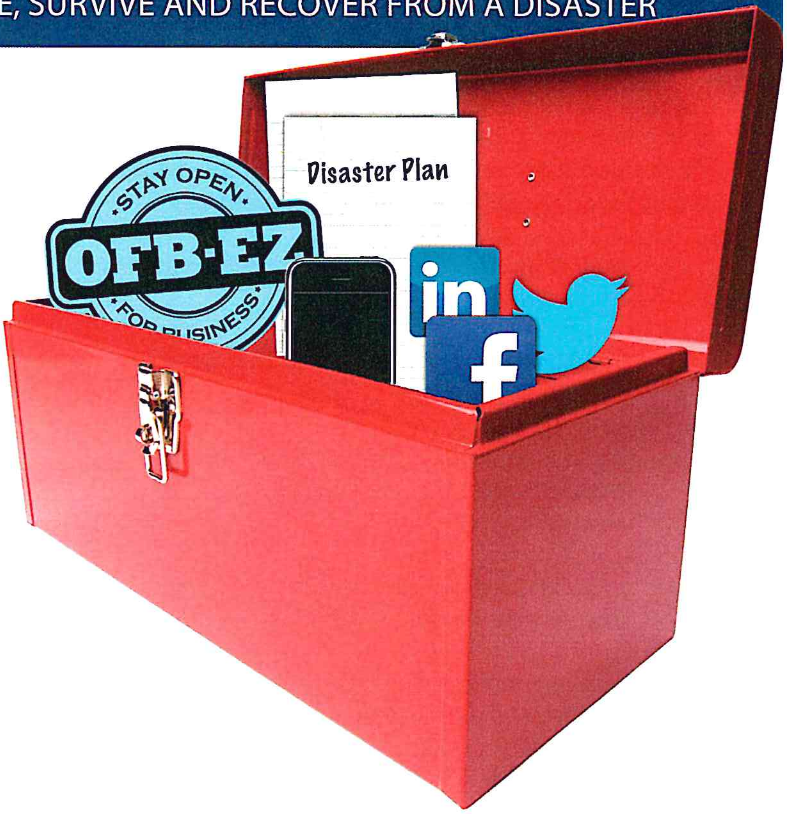
Insurance Institute for Business & Home Safety®

WHAT'S IN YOUR BUSINESS DISASTER RECOVERY TOOLBOX?

FIVE PLANS TO HELP YOUR BUSINESS PREPARE, SURVIVE AND RECOVER FROM A DISASTER

We are all too familiar with the images — business owners sifting through the rubble left after a disaster; food service firms coping with spoilage due to an extended power outage; retailers blocked from their customers due to a water main break which floods the street outside their location. As unfortunate as these events are, they do not need to result in a long, difficult recovery or worse, a permanent closure. In fact, many businesses successfully respond to and recover from natural disasters and other disruptions – in large part due to advance preparation and a planned response.

To effectively and successfully prepare for and respond to unexpected events, a business should have a recovery toolbox. It should contain the right tools to assist with the three phases of a disaster: preparing, responding, and recovering. The goal is to make sure all phases of a disaster have been considered and are incorporated into the business' plan. Discussed in this article are five types of plans that all businesses should have to ensure a successful disaster recovery.



PREPARE - Business Continuity Plan

A business continuity plan is a proactive strategy with a step-by-step process to minimize a business' downtime. It gathers needed information and defines the steps required to keep the business running during any type of disruption. These steps allow for continuation of critical business functions within an acceptable timeframe; provide clear and specific recovery responsibilities for key staff members; and assure access to resources such as technology applications, hardware, software, and vital records to respond to the business disruption. An effective business continuity plan also will identify a business' risks and threats, as well as ways to reduce the disruptions associated with those risks and threats. Documented workarounds and manual processes that should be executed by staff also are key to ensure critical processes are recovered in a timely fashion. The end result is a business that can continue to deliver its critical products and/or services at an acceptable level, even if there is damage to its physical location, inventory, or customary operations.

This tool is easy to find and put into practice. The Insurance Institute for Business & Home Safety (IBHS) has created OFB-EZ™, a free business continuity planning toolkit to help businesses translate professional continuity concepts into an actionable plan. By using OFB-EZ, a small business can take advantage of many disaster planning and recovery best practices without the need for a large company budget. OFB-EZ provides a simple eight-step process, which does not require users to be an expert in business continuity planning. To download OFB-EZ, business owners can go to www.disastersafety.org/open-for-business and start planning for the risks they face.

IBHS has partnered with member company EMC Insurance Companies to develop OFB-EZ Mobile. Find out more about the free app at www.disastersafety.org/blog/ofb-ez-goes-mobile/.

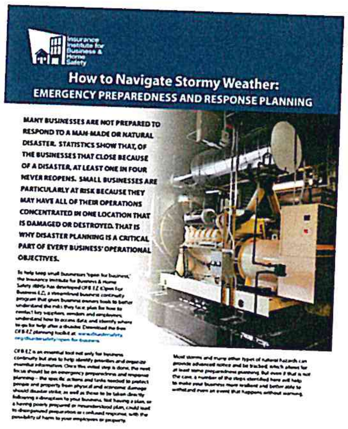
2 RESPONSE - Emergency Response Plan

An emergency response plan deals with immediate disaster response needs that are specific to a business' employees and work site, both during and after events such as severe weather, internal fire, chemical spills or other manmade disasters, civil disturbance, or building system failures. The same risk and vulnerability analysis that serves as the starting point for a business continuity plan will help focus an emergency response plan on things that matter most, and is the first step in this planning process.

The next step is to inventory the business' work site layout, structural features, and emergency systems in order to describe the detailed actions and steps to be taken immediately after a disaster or disruption. The main areas of focus are:

- protecting and ensuring the safety of employees and on-site visitors;
- initial inspection of buildings and surrounding areas for damage and hazards;
- damage control to minimize further impact to the business' assets (including buildings, any vehicles and equipment); and
- proper emergency notifications and internal (management and staff) communications.

As an effective planning tool, an emergency response plan should include detailed instructions about how to conduct each of these activities; key staff assignments, along with alternates or backups; and critical time intervals in which each activity should be undertaken. Because an emergency response plan will be activated in a time of crisis, it is important it is written in a way that is easy to understand and implement and kept in a place where it can be easily accessed when it is needed most.


Insurance Institute for Business & Home Safety

How to Navigate Stormy Weather:
EMERGENCY PREPAREDNESS AND RESPONSE PLANNING

MANY BUSINESSES ARE NOT PREPARED TO RESPOND TO A MAN-MADE OR NATURAL DISASTER. STATISTICS SHOW THAT, OF THE BUSINESSES THAT CLOSE BECAUSE OF A DISASTER, AT LEAST ONE IN FOUR NEVER REOPENS. SMALL BUSINESSES ARE PARTICULARLY AT RISK BECAUSE THEY MAY HAVE ALL OF THEIR OPERATIONS CONCENTRATED IN ONE LOCATION THAT IS DAMAGED OR DESTROYED. THAT IS WHY DISASTER PLANNING IS A CRITICAL PART OF EVERY BUSINESS' OPERATIONAL OBJECTIVES.

To help keep small businesses "open for business," the Insurance Institute for Business & Home Safety (IBHS) has developed OFB-EZ (Open for Business-EZ), a streamlined business continuity program that gives business owners tools to better understand the risks they face, plan for how to contact key suppliers, vendors and employees, understand how to access data and identify where to go for help after a disaster. Download the free OFB-EZ planning toolkit at www.disastersafety.org/disastersafety/open-for-business.

OFB-EZ is an essential tool not only for business continuity but also to help identify priorities and organize essential information. Once this initial step is done, the next focus should be on emergency preparedness and response planning – the specific actions and tasks needed to protect people and property from physical and economic damage should disaster strike, as well as those to be taken directly following a disruption to your business. Not having a plan, or a having poorly prepared or misunderstood plan, could lead to disorganized preparation or a confused response, with the possibility of harm to your employees or property.

Most storms and many other types of natural hazards can provide advanced notice and be tracked, which allows for at least some preparedness planning. But even if that is not the case, a number of the steps identified here will help to make your business more resilient and better able to withstand even an event that happens without warning.

Additional information on creating an emergency preparedness response plan is in IBHS' article "How to Navigate Stormy Weather: Emergency Preparedness and Response Planning" at www.disastersafety.org/commercial_maintenance/navigate-stormy-weather-emergency-preparedness-response-planning/.

3 RESPONSE - Crisis (Incident) Management Plan

Once an emergency situation is stabilized and basic operations have resumed, a crisis management plan helps a business move forward. It provides an organizational structure and brings together the right people to make critical decisions, such as prioritizing needed activities and resources and giving direction that will allow staff to work through a disruptive incident.

Although large companies often are able to structure a crisis management team from various areas of the business such as operations, I/T, human resources, communications, legal and finance, smaller businesses generally have to rely on team members who wear multiple hats—with one person serving as the leader. Team members (or at a minimum, the team leader) should be authorized to make decisions on behalf of the business in an emergency capacity.

While business continuity plans document how to continue offering a service or product and emergency response plans deal with staff safety and damage mitigation, a crisis management plan takes the next step beyond the initial emergency and details immediate actions that should be taken based on how the emergency is affecting people, property, operations, and reputation. The goal is to avoid panic, reduce confusion, and restore normalcy as quickly as possible. Additional information on creating a crisis management plan is available from the nonprofit Emergency Response and Crisis Management (ERCM) Technical Assistance Center at www.ercm.org/crisis-management-plan/.

4 RESPONSE - Crisis Communications Plan

Information is critical during a crisis; therefore, a crisis communications plan is essential for all businesses large or small. A crisis communications plan is very different from a crisis management plan; it describes how to process information related to the incident and then communicate it to the business' internal and external audiences. The plan's goal is twofold:

1. Maintain the business' brand and reputation by minimizing the repercussions due to untimely or misleading information; and
2. Ensure timely and accurate communications with all stakeholders (employees, the media, customers, suppliers and vendors, key business partners, and the public).

A crisis communications plan identifies:

- Who to communicate with, and who should do the communicating/speaking;
- How to deliver the message, along with a means for communication (a telephone tree, an emergency

notification system, website update, news release, social media – Facebook, Twitter, Linkedin, a call-in number, etc.); and

- What to say and what materials are needed (standard responses and scripts, message templates based on the nature of the crisis/disruption, contact information for the business' internal and external parties, etc.)

Creating a crisis communications plan in advance of a disruption helps to minimize the likelihood of misinformation, ease the communications burden, and increase the timeliness of messaging. Although every disaster has some unique features, thinking about crisis communications in advance allows the business owner to identify what is likely to be needed and make preparations, freeing up time to handle the actual disruption when it occurs. The plan should include strategies, policies, templates and detailed procedures on how and when to share information and with whom. The goal is to gather all critical information in one place, so it is easily accessed and consistently communicated.

5 RECOVERY - Information Technology Disaster Recovery Plan

Information technology (I/T) is a key component of most small businesses; therefore, it is necessary to have an I/T disaster plan in place to recover the business' I/T systems, data, and communications if a hardware or software failure or the destruction of the facility should occur. An I/T disaster recovery plan documents the step-by-step procedures to recover the systems, data (e.g., documents, files, records and reports) and applications in an orderly way, based on the pre-determined critical business processes identified in the business continuity plan.

In preparation for a possible technology failure, a business should inventory and document all hardware, software, and vital records (e.g., payroll, tax, accounting and production records). Electronic data should be backed up regularly and stored off-site and, where possible, hard copies of critical electronic files should be kept off-site. In addition, it is important to create a secure copy of computer and Internet log-in codes and passwords. Anticipating that computer equipment may be damaged or destroyed, it also is important to make pre-arrangements with I/T vendors to quickly replace damaged hardware and software.

Information on implementing an I/T disaster recovery plan is available from the Information Technology Disaster Resource Center (ITDRC) at http://itdrc.org/. The ITDRC is an established non-profit organization, and is comprised of hundreds of volunteer professionals from many technology disciplines. They provide small businesses with free resources to continue operations and recover their technology infrastructure following a disaster. IBHS has additional information in its article "Data Protection: A Vital Part of Business Protection" at www.disastersafety.org/commercial_maintenance/data-protection-a-vital-part-of-business-protection/.

ENHANCING THE TOOLBOX: ADDING A PANDEMIC PLAN

As a result of the current concern over the Ebola virus, as well as a predicted severe influenza season, many businesses are re-thinking their pandemic plans. This type of plan outlines strategies for avoiding a workplace outbreak and safely maintaining essential business operations if many employees are absent due to illness or caring for sick family members. Because a pandemic flu disruption can last many months, businesses should plan ahead to ensure they can provide critical products and/or services with a distracted or reduced workforce. This may include strategies to keep employees well, in addition to providing appropriate teleworking options for employees affected by the flu. For example, a social distancing policy which includes limiting face-to-face contact (e.g., encouraging communications by telephone or email, meetings by teleconference, no handshaking, increasing the physical distance between employees at the work site, or providing the ability to work remotely) can play a key role in protecting employees' health and safety and the viability of business operations.

The U.S. Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC) encourage businesses to plan for a pandemic. They have identified important, specific activities businesses can do to prepare in advance, including allocating resources to protect employees from contagions and establishing policies to account for absent employees. As is the case with all of the tools in the planning toolbox, it is critical to communicate with and educate employees, and to coordinate with external organizations and within the community.

Further information can be found at:

- www.pandemicflu.gov
- www.cdcfoundation.org/businesspulse/global-health-security

CONCLUSION

Planning for unexpected events does not guarantee everything will remain calm or glitches won't occur; however, having the right planning tools in place can help more smoothly guide a business through a disruption and its aftermath. Putting it all together – creating a complete toolbox – can help ensure your business becomes a success story rather than a picture of failure the day the unexpected arrives.

2014 COMMERCIAL SERIES

Insurance Institute for Business & Home Safety®

KNOWING YOUR RISKS:

THE STARTING POINT FOR BUSINESS PROTECTION AND BUSINESS CONTINUITY PLANNING

As a business owner, your job is to focus on how to expand your business and improve your profitability. It also is important to make time to examine your business' risks and vulnerabilities. When you have changes in your internal and external environments, your business may be exposed to new risks, and your tolerance for previously identified risks may change. That is why you should make conducting an annual risk and vulnerability assessment a priority, as part of your overall business protection planning.

AMONG THE QUESTIONS TO ASK YOURSELF EACH YEAR ARE THE FOLLOWING:

- What are the current high-risk activities conducted at your facility/location?
- Has your risk environment changed due to changes in your facility surroundings?
- Have you taken measures during the past year that have reduced some of your most common and likely risks?
- Have your tolerances changed so that less likely risks now should be considered a higher priority?
- Are there any new internal threats based on newly-installed equipment or newly-stored supplies on your premises?
- Are there any new external threats based on population changes, new transportation routes or types?
- Have you considered combinations of events and the possibility of one event causing another (cascading failures)?
- Can you put in place any new protection devices, safeguards or procedures to reduce your business' risks and hazards?
- Have you reviewed your insurance coverage with your agent?

Creating a business protection plan that is as unique as your operation is critical, because how you address potential threats may be very different from how another business handles its risks. This includes property protection, business continuity, and emergency preparedness and response for natural and man-made hazards. The plan should take into account your location, industry, company culture, business structure, management style, work functions, and even key business objectives. All of these affect how your organization chooses to protect itself from the threat of a business interruption, and how it will respond and recover should disaster strike.

The two biggest mistakes that many small businesses make are failing to identify a potential threat, and underestimating the severity of a known potential threat. Therefore, the starting point for most businesses to plan for a disaster is completing a **risk and vulnerability assessment** so that you know the risks you face now, how likely they are to occur, and what their consequences are for your business. This assessment is the process of identifying, quantifying and documenting the probability and overall potential severity of various types of threats or hazards (e.g., natural disasters or political events, human, technological or security factors, accidents or the loss of key staff) that could damage your facility and/or cause a disruption in your business.

DON'T BECOME A STATISTIC!

Research shows that

ONE IN FOUR

small businesses that close

due to a disaster will

NEVER REOPEN.

Anecdotally, the statistics are probably higher. Most surveys just cover the first two years after a disaster, and some businesses that do hang on only last two to five years before they give up. The best way to avoid becoming a statistic is to start business protection planning, or to update your plan if you already have one.

WHAT ARE THE COMPONENTS OF A RISK & VULNERABILITY ASSESSMENT?

1) IDENTIFY YOUR RISKS

The first step is to identify the possible natural and man-made hazards facing your business, both internal and external. For example, natural threats include hurricanes, floods, winter weather, and earthquakes, while man-made threats can range from a chemical leak to a widespread power outage (from either deliberate or accidental causes). Internal threats can involve employee misconduct, equipment failure, or an electrical fire, while external threats can come from the weather or a neighboring business. Regardless of the cause, a loss is a loss and the outcomes can be severe enough to force a business closure.

To help identify natural hazards that may affect your business' location, use the Insurance Institute for Business & Home Safety's (IBHS) ZIP Code tool at www.DisasterSafety.org. After entering your ZIP Code in the map's search box, you will receive a list of natural hazards in your area.

Another option would be to contact your local emergency management office for a copy of your community's hazards vulnerability analysis, which will include a list of potential natural and man-made hazards common to the geographic location of your facility.

Zip Code Risk Search Results
Search
EARTHQUA
Get your results at DisasterSafety.org
WILDFIRE

Identify natural hazards that may affect your business' location by using the IBHS ZIP Code tool available at www.DisasterSafety.org.

POTENTIAL RISKS FOR A SMALL BUSINESS

The following is a sample of potential risks to which your business may be exposed.

NATURAL

- Earthquake
- Tornado/Wind
- Hurricane
- Flood
- Volcanic Eruption
- Severe Winter Weather
- Wildfire
- Drought
- Sinkhole

POLITICAL

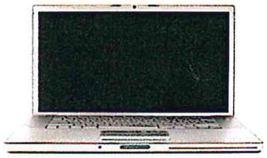
- Strike
- Riot
- Civil Disturbance
- Bomb Threat
- Biological Threat
- Nuclear Threat
- Act of War

MAN-MADE

- Sabotage
- Product Tampering
- Scandal
- Workplace Violence
- Kidnapping/ Extortion
- Sexual Harassment
- Fraud/ Embezzlement
- Theft
- Arson
- Terrorist Attack

TECHNOLOGICAL

- Software Failure
- Hardware Failure
- Power Outage
- Data Corruption
- Synchronization Error
- Cooling System Failure
- Wiring/Cables Failure
- Mechanical Systems Failure
- Communications Failure



SECURITY

- Privacy
- Virus
- Hacker
- Data Theft
- Counterfeiter
- Cybercrime

ACCIDENTS

- Human Error
- Fire/Explosion
- Water Damage
- Building Collapse
- Environmental
- Contamination

SIGNIFICANT LOSS

- Key Employee
- Senior Leader
- Subject Matter Expert
- Key Supplier/Vendor
- Premises
- Key Equipment

OTHER THREATS

- Pandemic/ Epidemic
- Gas/Water Shortage
- Media Crisis
- Special Event
- Mismanagement
- Product Liability

2) MEASURE THE PROBABILITY OF THREATS

How likely is it to happen? Once you have identified your potential threats, measure the probability of each risk and hazard by assigning each one a score on a scale of 0 to 5. It is important to consider how each risk or hazard can adversely affect your business. Think about what has occurred during the past year, such as:

- What kinds of emergencies have occurred in your community? (e.g., fire, natural disasters, accidents, etc.)
- What has occurred because of your location? (e.g., leakage of hazardous material or waste, roof damage, etc.)
- What problems were caused by employee errors or equipment failures?

FREQUENCY SCORE

The likelihood that the event will occur.

1. Very Low, not likely to occur

2. Low, somewhat likely to occur

3. Occasional, moderate chance of occurring

4. High, likely to occur

5. Extremely High, very likely to occur

3) MEASURE THE SEVERITY OF THREATS

The next step is to make an educated guess about the potential impact of each threat if it became reality – the amount of damage the event is capable of causing. You can measure the damage by evaluating the potential duration of the event, its magnitude, and its distribution or the extent of its reach (i.e., just one floor of a building, the entire structure, a neighborhood, a city or entire region, etc.). After taking into account each potential incident's duration, magnitude, and distribution, assign a score on a scale of 0 to 5. In addition to considering what has occurred during the past year, consider how other types of events could affect your business and others around you. Be sure also to take in account damage to infrastructure (e.g., roads, bridges, electric power, etc.) that could affect your ability to resume operations, and possible workarounds to expedite recovery.

SEVERITY SCORE

The amount of damage the event is capable of causing your business.

1. Very Low, minimal impact

2. Minor, low impact

3. Moderate, considerable impact

4. Significant, very high impact

5. Catastrophic, disastrous impact

4) MULTIPLY THE PROBABILITY AND SEVERITY SCORES FOR EACH THREAT

Once you have measured the probability and severity levels for each threat, multiply the values and record their totals. The highest ranking threats (score of 17 – 25) are those you will want to plan for as soon as possible. You should assume a high likelihood those hazards will strike your business and determine what controls you can put in place or could implement to minimize your risk. You can brainstorm how to manage or deal with those risks by considering:

- **Avoiding the Risk:** Deciding not to undertake an action due to the threat posed by the accompanying risk(s);
- **Mitigating the Risk:** Developing policies, procedures, and infrastructure to substantially reduce the likelihood of occurrence or severity of the risk;
- **Transferring the Risk:** Deciding to offload some or all of the risk using insurance or outsourcing, for example, in an effort to reduce the risk to an acceptable level; or
- **Accepting the Risk:** Deciding to accommodate a certain level of risk as part of your overall business strategy.

BUSINESS CONTINUITY PLANNING: WHERE/HOW DO I BEGIN?

To get you started, IBHS has created OFB-EZ™ (Open for Business-EZ), a free business continuity planning toolkit, to help you with recovery, re-opening faster, and reducing losses after a disaster or emergency. OFB-EZ assists business owners with essential activities, such as keeping in touch with key suppliers, vendors and employees; making sure their IT systems can function; and improving their ability to make quick, informed decisions after a disaster. The OFB-EZ toolkit also provides a section for business owners to better understand and evaluate the risks they face and the extent of their business' vulnerability to disruptions. Download the toolkit at www.DisasterSafety.org/open-for-business.

Creating a plan is only the first step in disaster preparation. Once you have identified the risks and vulnerabilities facing your business, the next step is to seek out the appropriate protective and mitigation measures specific to each type of interruption.

PROPERTY PROTECTION MEASURES

In addition to helping businesses identify their natural hazards, the IBHS ZIP Code tool at www.DisasterSafety.org also provides links to "how to" and "do it yourself" property protection projects that can help reduce the chances of loss at your business. The website also includes a video gallery showing how to perform many of these relatively easy tasks, and other disaster planning resources for small businesses.

As the IBHS Zip Code tool demonstrates, there are weather hazards that threaten specific regions (e.g., winter weather, wildfire), as well as those that affect all parts of the country (e.g., high winds, flooding, and loss of electrical power). Planning for the protection of physical assets through a well-documented and thorough emergency plan can greatly reduce the severity of an event to your business. For general information on severe weather planning, see IBHS' *How to Navigate Stormy Weather: Emergency Preparedness and Response Planning* at www.disastersafety.org/commercial_maintenance/navigate-stormy-weather-emergency-preparedness-response-planning/.

In addition to property protection measures that are weather-related, consider both internal and external maintenance issues that could result in damage or loss to your facility. IBHS' commercial maintenance resources at www.disastersafety.org/commercial_maintenance offer guidance on a variety of ways to reduce the frequency and severity of potential damage.

DATA PROTECTION ESSENTIAL TO ANY BUSINESS PROTECTION PLAN

Regardless of the specific threats that you identify through your risk and vulnerability assessment, don't forget that you need to protect your electronic and paper information, such as contracts and personnel records. Keep paper documents in a fire-resistant cabinet, duplicate them and store them off-site, or scan them into a document management system.

Cyber-related crime has been steadily increasing. Though it typically affects banks and large retailers, hackers may take aim at your small business. Discourage employees from taping passwords on or around their desk or placing them inside drawers. Back-up your data to an off-site location, whether as a physical backup or in the cloud. Additional recommendations are available in IBHS' *Data Protection: A Vital Part of Business Protection* at www.disastersafety.org/commercial_maintenance/data-protection-a-vital-part-of-business-protection/.

By using the resources provided by IBHS, business owners will be better able to keep their doors open following any form of disaster, reduce their potential for loss, and recover more quickly should the worst happen. The starting point for business continuity planning and any mitigation measures you undertake is a risk and vulnerability analysis.

IBHS is a non-profit applied research and communications organization dedicated to reducing property losses due to natural and man-made disasters by building stronger, more resilient communities.

Insurance Institute for Business & Home Safety
4775 East Fowler Ave.
Tampa, FL 33617
(813) 286-3400
DisasterSafety.org

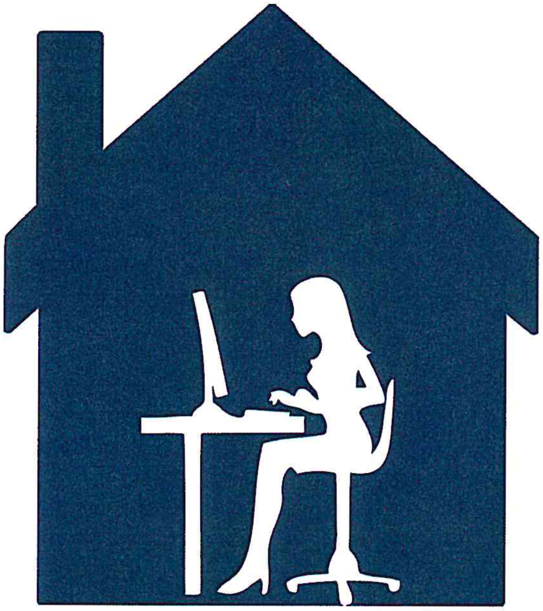
2015 COMMERCIAL SERIES

Insurance Institute for Business & Home Safety®

MAKE TELECOMMUTING PART OF YOUR BUSINESS CONTINUITY PLAN

What is telecommuting? Telecommuting is a growing workplace strategy that allows employees to work from home or any location away from the office, while staying connected through various I/T networks. Today, telecommuters make up a small but growing segment of the everyday workforce—growing nearly 80 percent from 2005 to 2012, and now representing about 3 percent of non-self-employed workers. However, beyond its routine function in the workforce, telecommuting can also be a vital option during a weather emergency or other workplace disruption.

This article looks at telecommuting as a key business continuity tool—one that enables businesses to maintain operations even if the workplace itself is shut down. While disruptions such as widespread power outages could still cause problems for some employees, telecommuting could help a business avoid a total shutdown by relying on remote employees to perform vital job functions. Highlighted here are some ideas about how business owners can include telecommuting in their business continuity plans, and what other considerations should be made before implementing this type of strategy.



BLIZZARDS, ILLNESS AND ROAD CLOSURES, OH MY!

The winter of 2014–2015 has brought record snowfalls in the Northeast and early snowfalls as far south as South Carolina. While the snow will eventually melt, telecommuting is a useful way to keep employees off dangerous roads, and also keeps employees from being stranded at work. In the case of a severe outbreak of influenza or other illness, telecommuting can separate healthy from potentially contagious employees to help maintain productivity and reduce anxiety. Similarly, telecommuting in response to a localized infrastructure problem, such as a bridge or major road closure, allows employees to stay focused on work and not on the difficulty of getting there. These are just a few examples of ways in which telecommuting can help businesses respond to emergencies.

IMPLEMENTING TELECOMMUTING AS A RECOVERY STRATEGY

For telecommuting to be a successful business continuity tool, businesses need to plan ahead by deciding which jobs are suitable for telecommuting, training staff, putting the right technology in place, addressing administrative challenges, and testing the new system. Listed here are a few considerations that should be well-thought-out in advance.

☑ IDENTIFY THE TELECOMMUTING FORCE

Telecommuting is an option only for employees whose jobs can be performed from a remote location, and only for employees whose work styles require minimal direct supervision. Generally, jobs that require significant onsite resources and equipment, hands-on service, or face-to-face interaction are not well-suited for telecommuting, while those that focus on reading, writing and analyzing, or are phone-intensive, are more suitable for telecommuting.

☑ MANAGE EMPLOYEE CONCERNS

When identifying only some employees for the telecommuting force, it is important to manage perceptions of unfairness—either for employees who think they would otherwise get a "free day" if the workplace were closed, or those who are required to physically report to work, even during adverse weather or other circumstances, while others are not.

☑ DOCUMENT THE TELECOMMUTE POLICY

When the office is closed because of a disruption, the business continuity plan should specify who is expected to work remotely and how the activation will take place, including the following considerations:

- Determine when and how employees will be advised not to come into the office and to begin working remotely.
- Determine how employees' time and attendance will be tracked, verified and controlled.
- Establish guidelines for employees for required communication by phone and email with their supervisor/manager.
- Decide whether to create a signed agreement stating what is expected of employees who telecommute during a disruption or emergency.
- Make sure telecommuting employees have an appropriate work environment in order to perform their job. The location needs to have safe working conditions and the employee must maintain protection of proprietary information, records, documents and equipment.

INFORMATION AND COMMUNICATIONS TECHNOLOGY REQUIREMENTS

As part of the planning process, appropriate technology for each job function must be put in place, including equipment, communications systems and security. Additionally, employees should document what is in place at their remote locations in order to provide and maintain I/T capabilities and support.

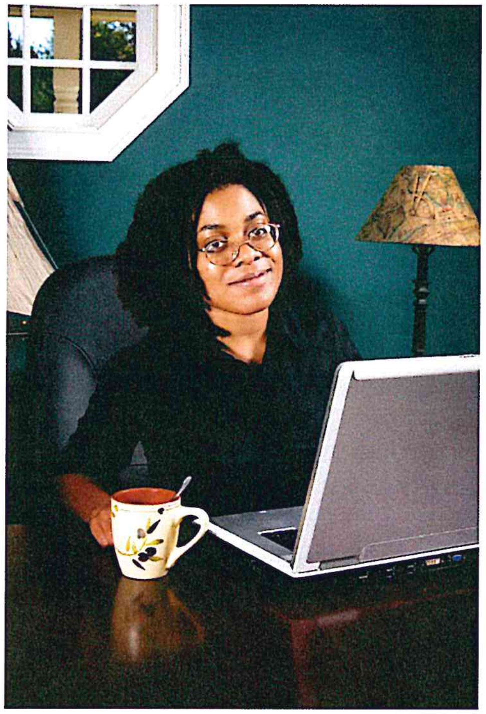
☑ EQUIPMENT

- If equipment is required, what will be provided by the business and what is the employee expected to possess?
- What expenses will be covered by the business (Internet, a second phone line for business calls, etc.)?
- What hardware is needed (e.g., desktop PC, laptop, tablet)?
- If the business issues supplies such as a laptop or tablet, what triggers when the employee must take it home to make sure it is available if needed?
- What software, applications, firewalls, antivirus and anti-spyware will be needed?
- Are there any other components necessary to do the job (e.g., printer, scanner, a particular operating system, UPS, etc.)?

☑ I/T INFRASTRUCTURE

- What type of Internet connection and/or bandwidth is required (broadband, DSL, cable)?
- What WIFI systems will be in place, and how can they be secured?
- What type of communication equipment is needed (phones, teleconferencing capabilities, tools like instant messenger, video conferencing and other online collaboration tools, etc.)?
    - o Determine how voice communications will be handled. Will the capability of rerouting the calls to employees' home or cell phones be available?
    - o Provide a list of contact information as a handy reference for telecommuting staff.
- Will access to remote help desk support be available to assist telecommuters with I/T issues?
- What type of training is necessary? Employees will need to be comfortable with the use of I/T systems (e.g., login process into VPN, etc.).

Lastly, it is important to establish practice and testing schedules. If employees do not work from home on a regular basis, the first few times may be confusing and difficult. Practicing and testing are key factors in having a successful telecommuting recovery strategy program available when needed.



Appropriate technology for each job function must be put in place, including necessary equipment such as a laptop.

TELECOMMUTING: NOT THE SOLE SOLUTION

When a disruption occurs, telecommuting can be critical to getting key employees productively working, but it is not a cure-all for all business recovery challenges. A severe natural disaster could damage many employees' homes or result in widespread power or communications outages. In these situations, business owners may want to consider the following more comprehensive approaches to relocation of employees.

- ✓ "Hot sites" are commercial workplace recovery facilities that have equipment readily available to address the business' critical needs. This may involve high monthly standby fees, and space may be limited as these types of providers do not have just one customer.
- ✓ "Warm/cold sites" are equipped with some of the business' needed equipment and may only be capable of providing backup after additional provisioning, software or customization is performed, generally at a lower standby cost.
- ✓ Memoranda of understanding (MOUs) or reciprocal agreements with a business ally that is accessible but not in the same risk zone may provide for shared office space or equipment if one company's workplace is inaccessible or inoperable.

After considering all of the advantages and disadvantages, choose a combination of the above alternatives to best meet the specific needs of the business.

INCORPORATING TELECOMMUTING INTO A BUSINESS CONTINUITY PLAN

The Insurance Institute for Business & Home Safety (IBHS) has created OFB-EZ®, a free business continuity planning toolkit to help businesses translate professional continuity concepts into an easy-to-use guide. By using OFB-EZ, a small business can take advantage of many disaster planning and recovery best practices without the need for a large company budget. To download OFB-EZ, go to www.disastersafety.org/open-for-business. Though the toolkit does not specifically include steps to incorporate telecommuting into the plan, the "Know Your Operations" and "Know Your Information Technology" sections can assist businesses with the necessary decisions for considering telecommuting as a possible solution. With the knowledge gained from completing an OFB-EZ plan, businesses can make an educated decision about whether telecommuting is a workable recovery strategy for them.

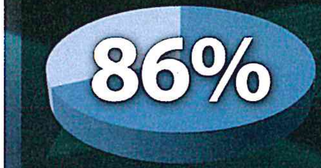
VIRTUAL PRIVATE NETWORKS (VPNs)

Providing secure access to the company's network is crucial for employees who telecommute during a disruption. A Virtual Private Network (VPN) is essentially a channel between the telecommuter and the office's local area network (LAN). When a telecommuter logs on through a VPN, he or she is routed to the company's internal network. From there, they can access drives and resources that are usually only accessible from inside the office. VPN access secures the Internet connection to guarantee all of the data being sent and received is encrypted and secured from unwanted eyes.

Keep in mind:

- Public WIFI networks are completely open and are not secure. If employees are permitted to use public WIFIs, have them use a VPN to guarantee security. Using a VPN encrypts communications no matter how or where they are connecting.
- If the VPN capacity is limited, implement a VPN login schedule (stagger access to eliminate sluggishness in speed). Staggering times during a workplace disruption—asking an employee to work late, start early or move their workdays around—to accommodate a VPN schedule is conceivable because employees are able to work from home.
- Not all VPNs are created equal. It is important to do research on the various options before selecting a VPN service/provider.

TELECOMMUTING BY THE NUMBERS

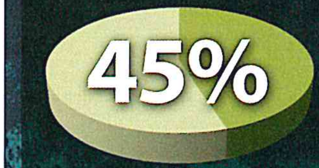


In 2009, a leading research and advisory firm conducted a survey which asked 285 business continuity/disaster recovery decision makers if their company had strategies for workforce recovery in their business continuity plans. 68% said yes. Of that 68%, 86% indicated they use remote access procedures as part of their strategy.

blogs.forrester.com/stephanie_balaouras/09-04-29-swine_flu_what_it_means_it_professionals

Three out of four teleworkers say they could continue to work in the event of a disaster compared to just 28% of non-teleworkers, according to a study conducted by an independent research firm that consults on emerging workplace issues and opportunities.

globalworkplaceanalytics.com/resources/costs-benefits



In late 2014, a company that offers software for remote access solutions conducted a survey of 916 employed people from five U.S. cities: Houston, Los Angeles, Miami, New York City and San Francisco. They found that despite the importance of information to most businesses and the push toward flexible work environments and mobile workforces, 45% of all respondents lack the ability to access company information from offsite locations.

www.hobsoft.com/solutions/HOB_Business_Continuity_Survey.jsp

IBHS is a non-profit applied research and communications organization dedicated to reducing property losses due to natural and man-made disasters by building stronger, more resilient communities.

Insurance Institute for Business & Home Safety
4775 East Fowler Ave.
Tampa, FL 33617
(813) 286-3400
DisasterSafety.org

2014 COMMERCIAL SERIES

Insurance Institute for Business & Home Safety®

SUPPLY MANAGEMENT:

REDUCING THE WEAK LINKS IN YOUR BUSINESS' SUPPLY CHAIN

The first step in business continuity planning is to identify and evaluate the possible risks facing your business. This should start with the natural hazards that are prevalent in your region (e.g., hurricanes, floods, winter weather, or earthquakes), along with other disruptions that might occur in your community, such as a chemical leak or a major power outage. More information on risk and vulnerability analyses can be found at: www.disastersafety.org/commercial_maintenance/knowing-risks-starting-point-business-protection-business-continuity-planning.

However, because almost every business relies on a chain of critical suppliers and customers, your business continuity plan needs to look beyond your immediate location to consider national or even global problems that can adversely affect your business. In fact, supply chain interruptions can happen anywhere, anytime—and sometimes you may not even be aware that a problem has occurred in a distant location until it reaches your business. Fortunately, your business continuity plan will help you prepare for unexpected supply chain problems, wherever they occur, and reduce the likelihood of disruption to your business. This article provides ideas on how best to address and plan for supply chain vulnerabilities.

SUPPLY CHAIN:

The movement of materials as they flow from their source to the end customer.

THE IMPORTANCE OF A STRONG SUPPLY CHAIN

According to a recent study, almost half of corporate insurance experts surveyed listed business interruption relating to supply chains as the top risk for businesses.[1] For most businesses, supply chains are not just a few isolated vendors and suppliers; in today's economy, they typically involve a web of third parties, including product distributors, service providers, manufacturers, contractors, and logistics firms that move materials (e.g., transportation, warehousing, and inventory management). In turn, all of them are dependent on their own infrastructure, such as electric and utility providers, Internet vendors, telecommunications suppliers, and transportation—and their supply networks. A broken link in any part of the supply chain can cause a domino effect that ultimately affects you.

As is so often the case, knowledge is power when it comes to supply chain management. Knowing the extent of your critical suppliers' preparedness for business disruption, and having alternate sources for supplies, manufacturing, and transportation needs when your primary supply chain is unavailable, is an essential part of your business continuity plan. This holds true for your upstream and downstream supply chain. Though this article speaks primarily to upstream supply chain management, you should be just as aware of your downstream supply chain, or where your profits come from (transactions and money spent by customers and clients). If a disaster in your region causes your customers to evacuate the area, you may need to consider expanding your product or services into new regions or to offer your product or services online to customers thousands of miles away.

Keep in mind that you may be a customer and a supplier at the same time. Just as you rely on your supply chain, others rely on you as part of their supply chain. Consider these following questions to determine what others may need and expect from you and what issues you should address with your current and potential suppliers. By focusing on these questions, you will have the ability to respond to your supply chain partners when they ask about your business' readiness, and you will have the information needed to select only those suppliers that you can clearly depend upon.

IDENTIFYING KEY LINKS IN YOUR SUPPLY CHAIN

The first step in testing the strength of your supply chain is to identify your critical suppliers and prioritize their importance to your operations based on the disruption that would occur should they encounter problems. Questions you should answer:

- Which products or services do you most depend on for your success – for profitability, reputation, and competitive advantage? Who are the suppliers?
- Do you have any time-sensitive activities, services, devices or systems whose failure or disruption would severely interrupt your business operations? Who are the suppliers?
- Are there specific products or services for which your supplier's inability to deliver goods or services would cause a bottleneck in your operations? Who are the suppliers?
- Do you have any suppliers who are *sole source providers* of goods or services (i.e., you can only get what you need from that one, particular supplier)? What alternatives do you have if they cannot deliver or go out of business?

UPSTREAM SUPPLY CHAIN:

Businesses that YOU depend upon to design, produce and supply your products or services to your customers or clients.

DOWNSTREAM SUPPLY CHAIN:

Your customers and clients, or the individuals and companies who purchase your products or services.

[1] The Allianz *Risk Barometer on Business Risks 2014* survey was conducted among risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of both Allianz Global Corporate & Specialty and local Allianz entities. http://www.agcs.allianz.com/about-us/news/press-riskbarometer2014/

EVALUATING YOUR SUPPLY CHAIN LINKS

Once you have identified your key supply chain links, you should assess their vulnerability to natural and man-made hazards, and confirm that they have business continuity plans in place.

Questions you should answer:

- Where are your key suppliers located and what natural and man-made risks are they likely to face? Are they based in a single location or have they diversified their risk with multiple locations?
- Do your key suppliers have a business continuity plan? In particular, verify how your suppliers can redirect their business to fulfill your needs for a product or service if they experience a disruption.
- Have any of your suppliers experienced an interruption in the past five years? If so, how did they respond, and how did the interruption affect their customers/clients?
- Do you have pro-active, close relationships with their key suppliers so that you will be aware of problems they may face and can work with them to minimize potential disruptions?
- Should you ask key suppliers to stockpile an item or ingredient to ensure they will have the capability of providing it to you, despite any interruptions?
- Can you identify other ways to minimize possible supply chain disruptions, such as "failure to perform" clauses in my contracts?

ADDITIONAL WAYS TO STRENGTHEN YOUR SUPPLY CHAIN

- o Make sure you have a good process in place for selecting the best and most reliable suppliers for your business. The cheapest is not always the most reliable.
- o Develop closer business relationships with your key suppliers – get to know them – including understanding their business' issues and challenges.
- o Remember that a single supplier may reduce paperwork, but multiple suppliers may reduce your vulnerability to supply chain problems.
- o Communicate regularly with your staff to understand the early warning signs of supplier trouble (e.g., lengthening cycle times and delivery times, top management changes, etc.).
- o Closely monitor regions where natural and man-made disasters hit and determine which of your suppliers are located in the area and if they are affected.
- o Involve your key suppliers in your business continuity planning, maintenance, and exercises, so they understand their role in your business.
- o Make sure your suppliers create and maintain robust business continuity plans, along with adequate insurance (ask to see their insurance certificates and, where possible, be named as an additional insured).
- o Develop plans to address supply chain risk situations when they inevitably do occur, including establishing relationships with alternate vendors and suppliers to provide redundancy for critical goods and services when needed.

REDUCING THE POSSIBILITY OF CASCADING FAILURES IN YOUR SUPPLIERS

Just as you rely on your supply chain for critical products and services, your suppliers must manage their own supply chain risk. Because of the many interdependencies of the supply chain, more and more businesses are taking steps to ensure their suppliers also manage their supply chain risks. In addition to verifying they have a business continuity plan, encourage them to identify and assess their own supply chain risks and take steps to reduce them.

CONCLUSION

A disruption in your supply chain can result from numerous factors, including natural hazards, power outages, transportation failures, and other unexpected events. The chances of any specific problem occurring will vary by business, sector, and geography, but the probability that your supply chain will be affected by at least one of them is high. With this in mind, it is important to recognize that your supply chain is a critical part of your business and should be included in your business continuity planning.

To help business owners create these plans, the Insurance Institute for Business & Home Safety (IBHS) developed OFB-EZ™ (Open for Business-EZ), a free business continuity planning toolkit to help you recover, re-open quickly, and reduce losses from a business disruption, available at www.disastersafety.org/open-for-business. OFB-EZ includes an exercise to help you identify and maintain contact information for key suppliers and vendors. This is the first step in incorporating supply chain management into your business continuity planning, and can help you restore your critical business operations and work processes following a disaster.

Recognizing that a chain is only as strong as its weakest link, it is important to select suppliers who take a "best practices" approach to risk management and business continuity planning. Identifying the right suppliers and strengthening your links will help you to stay in business not only when natural and man-made hazards affect your business, but also when suppliers thousands of miles away are at risk. Planning for supply chain disruptions will reduce your business' vulnerability and provide you with a competitive edge in our global economy.

★ STAY OPEN ★

OFB-EZ

★ FOR BUSINESS ★

Prepared by the Insurance Institute for Business & Home Safety (IBHS), which is an independent, nonprofit, scientific research and communications organization supported by the property insurance industry. The Institute works to reduce the social and economic effects of natural disasters and other risks on residential and commercial property by conducting building science research and advocating improved construction, maintenance and preparedness practices.

THE EASY WAY TO PREPARE YOUR BUSINESS FOR THE UNEXPECTED.

Insurance
Institute for
Business &
Home
Safety®

Contents

Overview

The Insurance Institute for Business & Home Safety (IBHS) has developed a new streamlined business continuity program for small businesses that may not have the time or resources to create an extensive plan to recover from business interruptions. IBHS is a leading national expert on preparing for, and repairing, rebuilding, and recovering from catastrophes both large and small. IBHS' mission is to conduct objective, scientific research to identify and promote effective actions that strengthen homes, businesses, and communities against natural disasters and other causes of loss.

IBHS' original business continuity program is called Open for Business®, or OFB. The new program, OFB-EZ®, is designed to be simple to use, administer and implement. With OFB-EZ, you can follow the same disaster planning and recovery processes used by larger companies – but without a large company budget. OFB-EZ is user-friendly and does not require any previous experience with or knowledge of business continuity planning.

This toolkit will help you:

1. identify the business activities that are essential for continued operation during a disruption;
2. deal with risks your organization faces; and
3. create an easy-to-use recovery plan tailored to your business, giving you confidence if the worst occurs.

Statistics show that one in four businesses forced to close because of a disaster never reopen. Small businesses, which form the backbone of the United States economy, are particularly at risk. IBHS' ultimate goal is for every small business to prepare a plan that will enable them to withstand and recover from any type of disruption.

Know Your Risks

Knowing your risks will help you evaluate the extent of your business' vulnerability to disruptions.

How potential threats impact each business varies considerably because no two businesses are exactly alike. Differences in location, industry, culture, business structure, management style, work functions and business objectives affect how you choose to protect your business from threats and how you respond to and recover from a business disruption.

The two biggest mistakes many small businesses make are failing to identify a potential threat, and underestimating the severity of a known potential threat. After completing the risk assessment, you will be able to determine the greatest threats to your business, the likelihood or probability for each of those threats, how severe each event could be, and the potential impact on each business function or process.

Identify Your Threats.

Use the Vulnerability and Risk Assessment to determine the threats that are likely to affect your business. Add any additional threats you are exposed to that are not already listed.

Rank the Probability of Threats.

How likely is it to happen? Assign a rank of 0 to 5 in the Probability Level row.

Rank the Severity of Threats.

You will need to assess the potential impact of each threat, which means the amount of damage the event is capable of causing. To measure the potential damage, think about the duration, magnitude, and the extent of the potential threat's reach (e.g., just one floor of your building, the entire structure, a neighborhood, the entire region, etc). After assessing all these factors, assign a rank of 0 to 5 in the Severity Level row.

Multiply the Probability and Severity Scores for Each Threat.

Once you have ranked the probability and severity levels for each threat, multiply values and record the total in the Total Value column.

The highest ranking threats (17-25) are those you will need to plan for as soon as possible. You should assume those hazards will strike your business, and determine what controls you have in place or could implement to minimize your risk.

RECOMMENDATIONS:

For a list of natural hazards that may affect your business' location, use the Insurance Institute for Business & Home Safety's (IBHS) ZIP Code tool to identify hazards in your area, and generate a customized list of projects that can reduce your risk.

You also should consider damage to infrastructure (e.g., roads, bridges, electric power, etc.) that could affect your ability to resume operations, and develop possible workarounds to expedite recovery.

In addition, contact your local emergency management office to obtain a copy of your community's hazards vulnerability analysis for a list of possible natural and man-made hazards that could affect your area.

About the Form

You should review and update your Vulnerability and Risk Assessment every six months. You will find that new ideas or considerations will surface each time, helping you refine your thinking and modify your plan. It is important to establish a maintenance program to keep your plan's contents current and relevant.

*MAKE COPIES OF THIS FORM

Know Your Risks

Use this form to review potential threats. Fill in one field for probability and one field for severity. Finally, multiply the probability and severity levels and enter the total in the total value column.

THREATS	Probability (0-5)	Severity (0-5)	Total
Earthquake			
Tornado/Wind/Hurricane			
Flood			
Severe Winter Weather			
Interior Fire			
Wildfire			
Loss/Illness of Key Staff			
Workplace Violence			
Software/Hardware Failure			
Power Outage			
Loss of Utilites (water, gas, electricity, etc.)			
Pandemic/Epidemic/Flu			
Loss of Premises			
Other			
Other			
Other			
Other			
Other			
Other			

Know Your Operations

Your ability to respond quickly to any type of business disruption could make the difference between survival and closure.

Determine the maximum amount of time you can endure being closed after a disaster occurs by identifying your key business functions and processes, and decide how long you can go without being able to perform them.

Consider the following:

- What is your main product/service?
- How do you produce this product/service?
- What are the things that could most likely impact your ability to do business?
- If your business were impacted, who would you need to call? How would you reach them?
- What other business functions and processes do you perform to run your overall business?
- Which of these business functions and processes have legal, contractual, regulatory or financial obligations?
- Can the function be performed off-site? What equipment is needed?
- How much downtime can you tolerate for each function?
- What are the consequences if the function cannot be performed?
- Can your business survive without a specific function?

RECOMMENDATIONS:

Think about your employees and what activities they perform on a daily, weekly, monthly, and annual basis. Think about the functions and processes required to run your business in: accounting/finance; production/service delivery; sales/marketing; customer service; human resources; administration; information technology; and purchasing.

About the Form

Rate each function with a priority level of Extremely High, High, Medium or Low, and complete a separate form for each one. Consider any workarounds methods or possible backups for each function. Determine whether there are any temporary processes that can be implemented until a permanent solution is available. Document detailed procedures for workarounds, including any additional resources required. It is important to establish a maintenance program to keep your plan's contents current and relevant - review your business functions and processes every six months.

*MAKE COPIES OF THIS FORM

Know Your Operations

Use this form to identify what business functions are critical to your business' survival. Duplicate the form for each business function.

Updated:

Next Review Date:

BUSINESS FUNCTION:

Priority: □ Extremely High □ High □ Medium □ Low

Employee in charge:

Timeframe or deadline:

Money lost (or fines imposed) if not done:

Obligation: □ None □ Legal □ Contractual □ Regulatory □ Financial

Who performs this function? (List all that apply)

Employees:

Suppliers/vendors:

Key contacts:

(For additional space, use the Notes area below)

What is needed to perform this function? (List all that apply)

Equipment:

Special Reports/Supplies:

Dependencies:

(For additional space, use the Notes area below)

Who helps perform this function? (List all that apply)

Employees:

Suppliers/vendors:

Key contacts:

(For additional space, use the Notes area below)

Who uses the output from this function? (List all that apply)

Employees:

Suppliers/Vendors:

Key Contacts:

(For additional space, use the Notes area below)

Brief description of how to complete this function:

Workaround methods:

Notes:

Know Your Employees

Your employees are your business' most valuable asset. Suppose an emergency prevents access to your business.

- Would you know how to reach your employees?
- Do you have current home and mobile telephone numbers, addresses, email addresses, and emergency contact information?
- Is your employees' contact information available outside your business location?

Current employee contact information will enable you to reach employees to determine their safety and whereabouts, inform them about the status of your operations, where, when and if they should report, and what to do following a disaster.

Two-way communication with employees is critical before, during and after a disaster. Create an employee telephone calling tree and an emergency call-in voice recording telephone number, and know how to email and text your employees. Designate a telephone number where employees can leave messages.

Determine what assistance is needed for employees with disabilities or special needs, such as communications difficulties, physical limitations, equipment instructions and medication procedures. Determine whether employees are caring for individuals with special needs, which could prevent them from being available during a disaster. Identify employees who are certified in First Aid and CPR, and those with special skills that could be helpful during emergencies.

Employee preparedness can make the difference between whether your business is able to effectively recover from a disaster or not. Encourage employees to make personal emergency preparedness plans. The more prepared your employees are at home, the faster they will be able to return to work to help your business respond and recover from a disaster.

RECOMMENDATIONS:

To maintain your communication readiness, have your employees review and update their contact information at least every six months. Create a special emergency email account using free services provided by Yahoo, Gmail, Hotmail, etc., to enable people to contact the company regarding their status. Be sure all employees know how to access the emergency account.

About the Form

Document employee contact and emergency contact information and key responsibilities. Is there someone who can perform these functions during an emergency? Make sure that special skills are not known by only one person. It is important to establish a maintenance program to keep your plan's contents current and relevant - review your employee contact information every six months.

*MAKE COPIES OF THIS FORM

STAY OPEN OFB-EZ FOR BUSINESS

Know Your Employees

Use this form to record information about all employees, including the business owner so that each person can be contacted at any time. Duplicate the form for each employee.

Updated:

Next Review Date:

EMPLOYEE NAME:

Position/title:

Home address:

City, State, ZIP:

Office phone: Ext. Alternate phone:

Home phone: Mobile phone:

Office e-mail:

Home e-mail:

Special needs:

Certifications:

□ First Aid □ Emergency Medical Technician (EMT) □ CPR □ Ham Radio

□ Other:

□ Special licenses:

Local Emergency Contact

Full name:

Relationship:

Home phone: Mobile Phone:

E-mail:

Out of State Emergency Contact

Full name:

Relationship:

Home phone: Mobile Phone:

E-mail:

Notes:

Know Your Key Customers, Contacts, Suppliers and Vendors

Preparedness planning is about being ready to manage any disruption to ensure the continuation of services to your customers. Your key customers need to know that you can provide "business as usual" even if others around you are experiencing difficulties. They will want to know that you are still in business or how soon you will be back and how the disruption will affect their operations. Maintaining up-to-date contact information for your key customers, contacts, suppliers, and vendors is critical.

The ability to resume your business operations relies on the capability of your suppliers and vendors to deliver what you need on time.

- Be sure your suppliers and vendors are not all in the same geographic location as you.
- Have alternate or backup suppliers and shippers in place.
- Request copies of your suppliers' business continuity plans.
- Establish a notification list and procedures.

Key contacts are those you rely on for administration of your business, such as:

- Accountant
- Bank
- Billing/Invoicing Service
- Building
    - Manager/Owner
    - Security
- Insurance Agent/Broker
- Insurance Company
- Internet Service Provider
- Payroll Provider
- Public Works Department
- Telephone Company
- Utilities

You may lose customers if you cannot meet their needs due to your own business disruption. After an event, it is important to keep customers informed about the status of your business, your product or service, delivery schedules, etc., and to develop mutually agreeable alternative arrangements.

RECOMMENDATIONS:

Identify various ways to communicate with customers after a disaster, such as direct telephone calls, a designated telephone number with a recording, text, e-mail, Twitter, Facebook, or announcements on your company website, by radio or through a newspaper.

About the Form

Be sure your customers know in advance how to obtain up-to-date information about the status of your business operations in the event of a disruption or major disaster.

*MAKE COPIES OF THIS FORM

Know Your Key Customers, Contacts, Suppliers and Vendors

Use this form to record information about your current suppliers, those you could use as an alternate choice and your key customers and contacts. Duplicate the form for each contact.

Updated:

Next Review Date:

CONTACT TYPE:

❏ Current Supplier/Vendor ❏ Back-Up Supplier/Vendor ❏ Key Customer/Contact

Company /Individual Name:

Account Number :

Materials/Service Provided:

Street Address:

City, State, Zip:

Company Phone:

Website:

Company Representative

Primary Contact:

Title:

Office Phone:

Mobile Phone:

E-mail:

Alternate Contact:

Title:

Office Phone:

Mobile Phone:

E-mail:

Notes:

Know Your Information Technology

Information and information technology (IT) are the lifeblood of most businesses, and must be included in your business continuity plan. Without access to your computer hardware, software, and digital data, your business operations can come to a standstill. It is likely that you communicate with or conduct business with your customers, partners, suppliers, and vendors via the Internet, which means your business is dependent on your computer system's connectivity and data communications.

Shut down and unplug all your computer hardware before an event to avoid serious damage due to power fluctuations. Consider elevating or moving equipment offsite. Have your employees take laptop computers home each day so they can work offsite if necessary.

Determine which data and records are vital to perform the critical functions identified in Know Your Operations section, and be sure they are backed up on one or more types of media. Store a backup copy onsite for use during small disasters, such as a failed hard drive, and store a second copy in a safe offsite location that can be easily accessed during large disasters.

Regularly backup your vital data and records. Move the backups to a different fire loss zone, safe deposit box or owner's home. The goal is to ensure your data and IT systems are available as you resume operations.

RECOMMENDATIONS:

Keep a backup copy of your computer's operating system, boot files, critical software, and operations manuals.

- Backup computer files, including payroll, tax, accounting and production records.
- Maintain an up-to-date copy of computer and Internet login codes and passwords.
- When possible, keep hard copies of critical virtual files offsite.
- Make arrangements with IT vendors to replace damaged hardware and software, and/or to set-up hardware and software at a recovery location.
- Request written estimates for rental or purchase of equipment, shipping costs and delivery times. Be sure to list these companies on your supplier and vendor form.
- When flooding is possible, elevate computer equipment stored on the floor.

About the Form

If your computer equipment is damaged or destroyed, you will need to lease or purchase new hardware and replace your software. Make a list of everything you would need to order. The important thing is to know what is needed to perform your critical business functions. It is important to establish a maintenance program to keep your plan's contents current and relevant - review your information technology information every six months.

*MAKE COPIES OF THIS FORM

Know Your Information Technology

Use this form to list the computer equipment, hardware and software, vital records and your back up processes that you will need to fulfill your critical business functions. Duplicate the form for each item or record.

Updated:

Next Review Date:

TYPE:

❑ Computer Equipment/Hardware ❑ Computer Software ❑ Vital Records

Item:

Title and Version/Model Number:

Serial/Customer Number:

Registered User Name:

Purchase/Lease Price: $

Purchase/Lease Date:

Quantity (equipment) or Number of Licenses (software):

License Numbers:

Technical Support Number:

Primary Supplier/Vendor:

Alternate Supplier/Vendor:

Notes:

Name of vital record:

Name of Business Function Vital Record Supports:

Type of Media:

Is It Backed Up?

How Often is it Backed Up?

Type of Media for Backup:

Where is it Stored?

Can the Record be Recreated?

Notes:

Know Your Finances

The time to prepare your business' finances is before a disaster occurs. Preparing your business financially now so it is ready to respond, recover, and continue operating when a business disruption occurs is just as critical as knowing exactly what to do when disaster strikes.

Here are some disaster preparedness ideas to consider:

Have an emergency cash reserve fund.

- You may need cash in order to purchase supplies or equipment, or relocate your business temporarily.

Have credit available.

- If you don't have enough cash in your emergency fund, be sure to have a line of credit or a credit card available.

Identify financial obligations and expenses that must be paid.

- You should not assume that because your area got hit by a disaster your suppliers, vendors and creditors are aware of the situation and are automatically granting extensions. Items such as mortgage, lease, or rental payments may still need to be made even after a disaster strikes your business.

Consider creating a policy regarding payroll during and after a disaster.

- Payroll is often overlooked in business continuity planning. You should not assume that your employees will continue to work without pay during or after a disaster. Be sure your employees are aware of your payroll continuity plans ahead of time in order for them to plan for their personal financial obligations.
- Establishing clear strategies and procedures for controlling costs, reporting information to appropriate groups and clearly budgeting for and tracking what is actually spent during a significant disruption can have a positive impact on the business' bottom line performance and recovery.

RECOMMENDATIONS:

It is critically important to protect your place of business, your contents and inventory, and/or your production processes with adequate insurance.

- Evaluate your insurance policies and meet regularly with your insurance agent/broker to be sure you understand your coverage, deductibles and limits, and how to file a claim.
- Most policies do not cover flood or earthquake damage and you may need to buy separate insurance for those events.
- Consider a policy that will reimburse you for business disruptions in addition to physical losses.
- Consider business income (or business interruption) and extra expense insurance. Even if you have to close your doors for a limited period, the impact on your revenue and net income can be substantial.
- Consider adding contingent business income coverage to your basic policy to be sure you are covered for expenses and loss of net business income, as well as income interruptions due to damage that occurs away from your premises, such as to your key customers, suppliers or utilities.

About the Form

Use the checklist when creating your financial strategy for your business resilience. It is important to establish a maintenance program to keep your plan's contents current and relevant - review your finances every six months.

*MAKE COPIES OF THIS FORM

Know Your Finances

Use this checklist to consider and plan for your business' financial needs in the event of a disruption.

Updated:

Next Review Date:

Overall Business Needs

Have you worked with your bank to set up a line of credit for your company?

Who is responsible to activate it and who has access to it?

How much cash would be needed to survive a 3-day, 5-day, 10-day, or longer shutdown?

For what purpose is the cash needed?

Will you have that cash on hand?

Who would make the decision to utilize the cash?

Who would have access to the cash?

Do you have sufficient cash to pay for various additional services that might be needed, such as janitorial or security services?

Do you have a company credit card that could be used for emergency purchases?

Who is authorized to use the credit card?

Will you be able to pay your bills/accounts payable?

Do you have procedures in place to accommodate a business disruption?

Will you be able to continue to accept payments from customers/accounts receivable?

Do you have procedures in place to accommodate a business disruption?

Have you identified an alternate location where you can work?

Human Resources

In the event of a widespread disaster, how will payroll be handled?

If your business is forced to shut down temporarily, will some or all employees continue to be paid?

For how long?

Will they be able to use their sick and/or vacation time without restriction?

Are there union considerations?

Have your employees been made aware of your policies that will be in place during a disruption?

If banks are closed, will your business provide payroll-cashing services?

What is your business' policy on cash advances, check cashing, and employee loans?

Will your employees be expected to work overtime?

Know When to Update Your Plan

For your plan to be successful when a business disruption occurs, it needs to be continually maintained and updated. One effective way to do this is to include business continuity planning anytime there are changes in your business or your location – basically, in every business decision you make. Keep your employees up-to-date with any plan changes as this will help when they need to put the plan into action, which in turn will reduce the negative impact to your business.

Maintenance is fairly straightforward. Repeat the following process every six months:

- Have your employees review the plan.
- Is anything out of date?
- Has all contact information been verified and updated?
- Have your procedures changed?
- Have there been any changes in business priorities?
- Have responsibilities changed?
- Document any changes.

Finally, test your plan and conduct exercises with your key employees. Until you test your plan for vulnerabilities you may not see where the gaps are in keeping your business going during a disruption. No plan or set of documents should remain sitting on a shelf.

Conducting exercises or drills are effective ways to test your plan, engage employees and train them. The following pages include an exercise that deals with a power outage. Once you learn the basics of conducting an exercise, you can easily generate your own scenario.

Another option to test your plan is to pose this scenario to employees at the end of a staff meeting: "If the alarm in this building were to go off, we would exit the building. Once outside we are told that we cannot go back into the building for one week. What would you do? How would you continue to work?" This will get people thinking about the possibilities and get them on board with your program. You may be surprised at your employees' increased level of growth and maturity when it comes to making the correct decisions following a disaster. This type of exercise can also be a great team building activity.

About the Form

Disaster exercises provide opportunities for you to: test company disaster readiness; train employees through practice; improve employees' ability to make informed decisions when responding to an emergency; identify what needs to be done during and after a disaster; and examine a specific scenario or situation more closely.

Gather your team, key employees and anyone else who would benefit from the exercise, present the power outage scenario, and begin the discussion with the questions provided. This can be done informally, such as during lunch or as part of a staff meeting.

*MAKE COPIES OF THIS FORM

Know When to Test Your Plan
Table Top Exercise: Power Outage Scenario

It is a hot, rainy Friday morning. The current time is 11:30 AM. Suddenly, the lights go out and all of the computers, printers, and copiers turn off. For a few seconds, there is silence before the chatter begins to pick up. One of your emergency lights comes on, but the rest are not working. While many of the offices have windows to provide minimal light, the majority of the hallways and interior rooms are left in the dark.

1. Take the first 10 minutes to discuss what you will do next.

It is now 1:00 PM and the lights still are not on. The building HVAC has been off now for 1 ½ hours and the temperature inside the building is gradually becoming unbearable. Your entire power grid is without power. There is no word from the electric company about restoration of power.

2. Now what are you going to do?
3. Is your technology/computer room being dealt with? By whom?
4. Has someone turned off all computers, printers, and equipment to prevent electrical surge when power is restored?
5. Is your phone system down? How are you going to manage the phone lines?

It is now 2:00 PM. Employees are asking if they can leave early. The word around town is that the power might not be restored for several days.

6. How will you communicate this message? What instructions will you convey to your employees? Customers? Vendors?
7. Are you going to declare a disaster in order to activate your business continuity plan?
8. Continue your discussion with the following questions:
9. How are people within the organization communicating with each other (e.g., sending and receiving messages, information, and response details)? How are they communication with other stakeholders (e.g., your customers and clients, the media)?
10. Is there a pre-determined and agreed upon central meeting place for company leaders, management, and employees?
11. Is there a copy of your business continuity plan that you can easily retrieve?
12. Are there any business processes for which there are manual workarounds? If so, discuss how that would happen.
13. How would you find an appropriate place to operate from for the remainder of the day? For the next one or two weeks, if necessary?
14. Have you begun an assessment that includes an evaluation of the status of employees, customers, operations, and external utilities?
15. How would you ensure that customer concerns are managed?
16. Have you begun to determine how much data was lost and how that will affect your operations?
17. Some employees are asking, "How will I know if I should come to work Monday?"

*MAKE COPIES OF THIS FORM

Know When to Test Your Plan
Table Top Exercise: Power Outage Scenario

It is now 7:30 AM on Monday, three days later. The power is still out and the Health Department has determined that "no building without running water can open for business." Clients are calling and the company voicemail system is full. Employees are texting the Human Resources Director asking for guidance.

18. What do you tell them?

Exercise Debrief:

19. What is missing from your plan?
20. What worked well in this scenario?
21. What did not work so well?
22. What could you do differently next time that would improve your response?
23. List the actions you will take to improve your plans.

Exercise Wrap Up:

This completes the exercise. In order to maximize what can be learned from this effort, have all participants write down their thoughts and concerns. You can address these and the debrief issues at future meetings.

Notes ______________________________

Exercise Date: ______________

Next Exercise Date: ______________

Know Where To Go for Help

Your relationship with your community and outside agencies can strengthen your ability to protect your employees and property and return to normal operations. Maintain a channel of communication with community leaders, public safety organizations such as the police, fire and emergency medical services, government agencies, utility companies, and others. Working together with outside agencies can be beneficial because they can provide a wealth of information to help you recover quickly from a disaster.

Refer to the resources below for more information about implementing disaster safety recommendations to help you prepare for and recover from natural or other types of disasters.

Insurance Institute for Business & Home Safety

In addition to providing this free business continuity tool kit, IBHS provides free disaster preparedness and property protection guidelines, recommendations and projects for small businesses. The Institute also offers post-disaster recommendations on repairing and rebuilding to make your building(s) stronger and safer the next time a disaster strikes.

http://disastersafety.org

American Red Cross

Among other disaster preparedness and response services, the Red Cross offers a number of preparedness training programs and resources for workplaces, families, and individuals.

www.redcross.org

Business Civic Leadership Center – Disaster Help Desk

The BCLC Help Desk is designed to enhance community economic recovery after a disaster. The Help Desk provides on-the-ground coordination of information among businesses, local chambers of commerce, NGOs, government responders, and disaster recovery specialists.

http://bclc.uschamber.com/site-page/disaster-help-desk-business

DisasterAssistance.gov

Provides information on how you might be able to get help from the federal government before, during and after a disaster. If the President of the United States makes help available to individuals in your community after a disaster, you can visit this site to apply online.

http://www.disasterassistance.gov

Federal and Local Emergency Management Agencies

Even the largest, most widespread disasters require a local response. Local emergency management programs are the core of the nation's emergency management system.

http://www.fema.gov/regional-operations/state-offices-and-agencies-emergency-management

Internal Revenue Service–Disaster Assistance and Emergency Relief for Businesses

The IRS offers audio presentations about planning for disaster. These presentations discuss business continuity planning, insurance coverage, record keeping and other recommendations for staying in business after a major disaster.

http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Disaster-Assistance-and-Emergency-Relief-for-Individuals-and-Businesses-1

Small Business Administration

The U.S. Small Business Administration provides loans, loan guarantees, contracts, counseling sessions and other forms of assistance to small businesses following a disaster.

http://www.sba.gov/
http://www.sbaonline.sba.gov/services/disasterassistance/disasterpreparedness/

Small Business Development Centers

The SBDC assists small businesses with financial, marketing, production, organization, engineering and technical problems, as well as feasibility studies.

http://www.sba.gov/content/small-business-development-centers-sbdcs
http://www.asbdc-us.org/

Acknowledgments

The staff of IBHS wishes to acknowledge the valuable input of all those who assisted in producing this toolkit. In particular, we extend thanks to:

- Steve Elliot, President & CEO, Elliot Consulting
- Frantz Joachim, CBCP, Director of Risk Management, AmeriLife
- Tim Lovell, Executive Director, Tulsa Partners, Inc.
- Mark R Lupo, CBCP, Area Director, The University of Georgia SBDC of Columbia
- David Maack, CEM, CPM, WCEM, Coordinator, Racine County Office of Emergency Management
- Lisa Marino, CBCP, Enterprise Business Continuity Management, Mercury General Corporation
- Howard Pierpont, Chairman of the Board, The Disaster Preparedness and Emergency Response Association [DERA]
- Marcus Pollock, Chief, Standards and Technology, National Integration Center, FEMA, DHS
- James Price Jr., MBCP, MBCI, ITIL, CEO, 3J Contingency Planning Services
- Bob Roberts, Emergency Manager, Tulsa Public Schools
- Sonia Singh, Emergency Preparedness Coordinator, City of Markham, Canada
- Judith Warren, Regional Coordinator, Humboldt State University, Office of Distance and Extended Education

Feedback

IBHS welcomes your feedback and comments about the OFB-EZ recovery planning toolkit, including the usefulness of your plan when a business disruption or workplace disaster occurs. Your feedback will help IBHS improve the tool for future users, and your story may help encourage others to develop a business continuity plan. Please send any feedback to info@ibhs.org.

OFB-EZ is a program of the Insurance Institute for Business & Home Safety
Download this document at DisasterSafety.org/open-for-business

BUSINESS CONTINUITY: MAKE PLANS INSTEAD OF EXCUSES!

Business disasters come in all shapes and sizes. Business owners should take steps now to give themselves a better chance to reopen quickly. Without a business continuity plan, one in four businesses forced to shut down because of a disaster never reopens.

STAY OPEN
OFB-EZ
FOR BUSINESS

TURN EXCUSES INTO ACTION

Businesses have lots of excuses for not having a business continuity plan, including the most common "we thought it would never happen to us." The following are common misperceptions about business continuity planning:

- Creating a plan takes too much time
- Creating a plan takes too much money
- We thought we had no risks
- We had more important things to think about
- We thought our Internet technology was fine
- We thought we could deal with a crisis when it happened
- We thought we were too small to need a plan
- We couldn't find the right solution
- We already backed up our data and thought that was the same as business continuity
- We didn't know where to go for help

TIME IS MONEY.

OFB-EZ is designed to help small businesses focus on planning for any type of business interruption, so they can get a jump start on recovery, re-open faster, and reduce their losses. A short summary of the 8-step process follows.

Insurance
Institute for
Business &
Home
Safety®

Find out more at DisasterSafety.org/open-for-business

If any of these sound familiar, it's time to stop making excuses and start making plans. While there are quite a number of business continuity solutions available, a good place to start is with the free, easy-to-use OFB-EZ™ (Open for Business-EZ) toolkit created by the Insurance Institute for Business & Home Safety (IBHS). OFB-EZ takes business owners step-by-step through the planning process in order to create a plan that helps them to:

☑ IDENTIFY RISKS

Focus on the risks that are most likely to disrupt their business operations.

☑ IDENTIFY CRITICAL FUNCTIONS

Identify the activities that are essential for staying in business and recovering quickly.

☑ BUILD A PLAN

Create an easy-to-use recovery plan tailored to specific needs.

ABCS OF WHY CONTINUITY PLANNING IS IMPORTANT

There are many good reasons for businesses to plan for the unexpected, most importantly protection and preserving the bottom line. To keep it simple, remember the ABCs:

AVOID MARKET SHARE LOSS

With a business continuity plan, your business will have a better chance of remaining competitive and minimizing the loss of revenue and customers. A solid and tested plan boosts customer confidence. When your customers know you have plans in place to provide continued delivery of goods and services during a crisis, they are less likely to flee to competitors if a disaster threatens your area.

BRAND PROTECTION

Having a plan allows you to demonstrate that your business is committed and prepared to protect your employees, clients and their assets at all times. This demonstrates a proactive attitude and can enhance employee morale and public opinion about your business. With increased confidence in your business' ability to operate during unexpected circumstances, your positive reputation grows with customers, staff, partners and investors.

COMMUNICATIONS

Having a business continuity plan will improve communication within your organization and with customers, suppliers, vendors, and key stakeholders. This is a helpful way to improve daily operations, not only in the event of disaster.

BASIC ELEMENTS OF A BUSINESS CONTINUITY PLAN

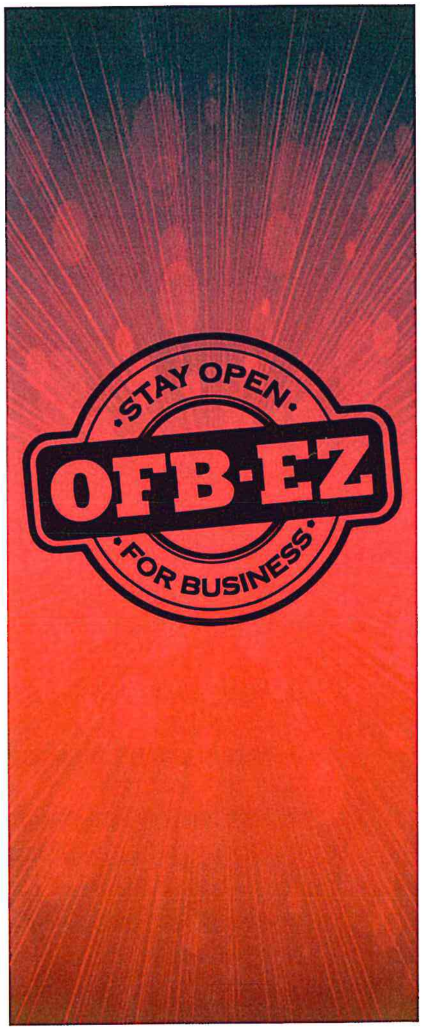
OFB–EZ translates professional business continuity concepts into common business language, through a streamlined eight step process. Here's how businesses can make it happen:

1. Know Your Risks
2. Know Your Operations
3. Know Your Employees
4. Know Your Suppliers, Vendors, Key Customers, and Key Contacts
5. Know Your Information Technology
6. Know Your Finances
7. Know When to Update and Test Your Plan
8. Know Where to Go for Help

GET STARTED NOW

Business continuity planning is vital to survival and should not be put off indefinitely as you focus on today's challenges. It's important to devote enough time and attention to planning for the future, even when that future may involve events that are unpleasant to think about and, hopefully, not likely to happen. Open for Business recognizes this and is designed to help you gather information, improve communication, and develop operational contingencies that will be useful today as well as tomorrow. So, stop making excuses and start making plans!

Visit DisasterSafety.org/open-for-business to download the free toolkit and begin your planning process today.



Insurance Institute for Business & Home Safety®

Find out more at DisasterSafety.org/open-for-business

DISASTER PLANNING MADE EASY

The Insurance Institute for Business & Home Safety (IBHS) has created a new disaster planning program for small businesses. Based on IBHS' Open for Business (OFB) program, OFB-EZ™ is a free business continuity tool translating professional business continuity concepts into common business activities, through a simple eight step process.

STAY OPEN
OFB-EZ
FOR BUSINESS

WHO SHOULD USE OFB-EZ?

Many businesses are not prepared to respond to a man-made or natural disaster. One in four businesses forced to close because of a disaster never reopens. Small businesses are particularly at risk because they may have all of their operations concentrated in one location that is damaged or destroyed. Although every business needs to prepare for potential disasters, OFB-EZ is designed so that those without professional risk managers or business continuity planners can easily understand what they need to do, and how to do it.

WHY USE OFB-EZ?

The OFB-EZ tool helps small businesses take the steps they need to keep functioning in the event of a major disaster or a smaller disruption. The goal is to continue to perform your most critical operations, which will help reduce short- and long-term losses to your bottom line.

Additional benefits are that you will be contributing to your community's resiliency by keeping your employees on the job and your goods and services available to your customers. The suggested planning exercises in the online tool are a great way to build teamwork, and make sure that all of your employees know what to do in the event of an emergency.

TIME IS MONEY.

OFB-EZ is designed to help small businesses focus on planning for any type of business interruption, so they can get a jump start on recovery, re-open faster, and reduce their losses. A short summary of the 8-step process follows.

Insurance Institute for Business & Home Safety®

Find out more at DisasterSafety.org/open-for-business

☑ KNOW YOUR RISKS

OFB-EZ starts by helping you identify the most serious threats to your business by focusing on what disruptions are most likely to happen, and what the impact would be if they do. This exercise will help you focus your planning on those threats with the highest risk (greatest likelihood X worst disruption).

☑ KNOW YOUR OPERATIONS

To focus your plan on the things that matter most to your bottom line, you also need to identify your key business functions and processes, and decide how long you can go without being able to perform each of them. OFB-EZ helps you do this by giving you a tool to document critical details for each business function, such as how quickly it needs to be restored, the people who perform the function, and who receives the output. As you think about these things, you will be asked to identify any IT resources needed to perform the function and any manual workarounds.

☑ KNOW YOUR EMPLOYEES

Almost every small business relies on its employees to succeed. That is why it is critical to know how to locate your employees after a disaster, make sure they are safe, and let them know about the status of your business operations and how they can get back to work. This can happen only if you have obtained and maintained current contact information for all your employees. OFB-EZ provides a convenient place to record basic employee contact information, as well as options for communicating with employees if phone and power lines are down. It is important to share your communications plans with employees before a disaster strikes.

☑ KNOW YOUR KEY CUSTOMERS, CONTACTS, SUPPLIERS AND VENDORS

Your key customers will want to know that you can provide "business as usual" even if others around you are experiencing difficulties following a disaster. They will want to know if your operations are running, or how soon you will be back in business, as well as the effect of your disruption on them. Having up-to-date contact information for your key customers, contacts, suppliers and vendors is just as important as knowing how to reach your employees. OFB-EZ allows you to create and maintain contact lists and keep them where they are easily accessible.

☑ KNOW YOUR INFORMATION TECHNOLOGY

Information and information technology are the lifeblood of almost every business. They also are extremely vulnerable to many disruption scenarios, ranging from a localized power outage to a major natural catastrophe. OFB-EZ helps you inventory and document your information technology, including hardware, software, digital data and connectivity. It also reminds users of the importance of frequent back-ups, off-site storage, and restoration options.

☑ KNOW YOUR FINANCES

The time to prepare your business' finances for a potential disruption is before a disaster occurs. To help business owners do so, OFB-EZ provides a checklist to assist in creating a post-disaster financial strategy, along with an inventory of key financial contacts. Although OFB-EZ is not an insurance program, it provides guidance on how to review your insurance coverage in regards to what is covered, what is not covered, and other available types of coverage.

☑ KNOW WHEN TO UPDATE AND TEST YOUR PLAN

Once you have documented your plan, distributed it, and trained your employees how to use it, you may think you are finished. However, your organization is constantly changing, and so is the environment around it. That's why it's important to update and test your plan regularly, using suggestions provided by OFB-EZ. It also is vital to recognize that disaster planning is not only a paper exercise, it needs to actively involve the people you will rely on in a real event. The "power outage" table top exercise in OFB-EZ is an effective way to test your organization's disaster readiness and learn where you need to improve.

☑ KNOW WHERE TO GO FOR HELP

OFB-EZ is a compact disaster planning tool, but there are many additional resources available that provide further disaster safety recommendations and aid in your recovery after an event. The online toolkit provides contact information for some of these organizations; there may be others in your local community. It's also a good idea to maintain a communications channel with community leaders; public safety organizations such as the police, fire and emergency medical services; local government agencies; utility companies; and others that may help you with disaster planning or recovery.

No matter what you do, or where you do business, disasters can strike, sometimes without a moment's notice. OFB-EZ will help you prepare for the unexpected, and respond should it actually occur. But it's not enough simply to read this article and think about being prepared. Now is the time to download the free OFB-EZ toolkit and start working on the plan that may help you survive, and even thrive, when the disaster you plan for becomes the disaster you recover from.