Nationwide®, a member of the Insurance Institute for Business & Home Safety, is proud to present you with valuable IBHS loss control resources.

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.

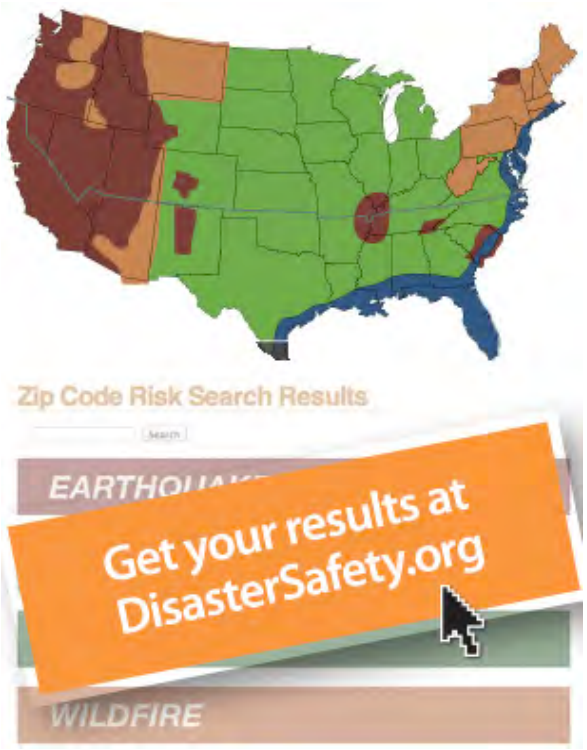
WHAT ARE THE COMPONENTS OF A RISK & VULNERABILITY ASSESSMENT?

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.



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?

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.

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

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.

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