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

Every Business Should Consider a Risk and Vulnerability Assessment

What risks truly threaten your organization? How will a business interruption impact your business functions? Will your business be able to recover and reopen once the disruption or disaster passes? These are the questions every small to mid-sized business owner should be asking and then seeking to answer.

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. However, there are ways to take control of the risks facing your business and avoid becoming a statistic. Creating a preparedness plan, practicing that plan, and putting it into action when the unexpected happens are important steps toward having less damage and shorter interruptions when an event does occur.

Creating a business continuity plan that is as unique as your operation is critical because how potential threats will impact your organization may be very different from how another business handles its risks. The plan should take into account your location, industry, company culture, organizational structure, management style, work functions, and even key business objectives. All of these can affect how an organization chooses to protect itself from the threat of a business interruption and how it will respond and recover.

Recognizing that there is no "one size fits all" approach, the starting point for most businesses to plan for a disaster is completing a Risk and Vulnerability Assessment. This is the process of identifying, quantifying and documenting the probability and overall severity of various types of threats or hazards (e.g. natural or political events, human, technological or security factors, accidents or the loss of key personnel) that could damage your facility and cause a disruption in your business.

WHAT ARE THE COMPONENTS OF A RISK & VULNERABILITY ASSESSMENT?

There are three basic components of a Risk and Vulnerability Assessment:

RISK ASSESSMENT

Identify the possible natural and manmade hazards, rank their probability and potential severity, then review the collected results to identify the most likely events that could happen. The two biggest mistakes that many businesses make are (1) failing to identify a potential hazard, and (2) underestimating the severity of a known potential hazard. For a list of natural hazards that may affect your business' location, visit the Insurance Institute for Business & Home Safety's (IBHS) website, enter your ZIP Code in the box on the map to identify regional natural hazards in your area, and generate a customized list of projects that can address property risks. You should also consider damage to infrastructure (e.g. roads, bridges, electric power, etc.) that could affect your ability to resume operations, and possible workarounds to expedite recovery.

RECOVERY PRIORITY ANALYSIS

Define the recovery priorities of your critical business functions through a more detailed analysis of recovery timeframes and analyze how those threats might impact your organization. In addition to your organization's critical business functions, you should identify your facility's structural and interior vulnerabilities. Taking precautions and making the necessary improvements will result in a more secure building and less business disruption.

ASSESSING THE VULNERABILITY

Combine the results of the Risk Assessment and the Recovery Priority Analysis and determine what strategies are necessary to avoid the risk altogether, reduce the possibility of loss, accept the risk and live with it, or transfer your risk to another party through the purchase of insurance or outsourcing of certain tasks. This is the first step in developing a plan to address each major threat to your business and expediting recovery after an event.

WEATHER IS JUST ONE ELEMENT OF RISK

For small to mid-sized businesses, a disaster is an event that disrupts business to the point that financial and operational consequences become unsustainable. Events come in all forms and are not necessarily weather related. Sometimes the event is man-made through deliberate or accidental causes, the result of a technological failure, pandemic flu or high absenteeism, or something as simple as a burst water pipe or disruptive as a power outage. Regardless of the cause, a loss is a loss and the outcomes can be severe enough to force a business closure.

WHERE/HOW DO I START?

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.

Get started with the IBHS Open for Business® toolkit, a free program to help small to mid-sized businesses develop a business continuity and property protection plan.

Using the tools provided by Open for Business®, business owners can begin the process to become more ready to keep their doors open following any form of disaster, reduce their potential for loss, and recover more quickly should the worst happen. Regardless of the cause of the business interruption, the ability to assess what needs to happen (and when) could be the difference between survival and closure.

The IBHS program offers worksheets and online training tools to help simplify the process. One of the advantages of using Open for Business® is the guidance to identify critical functions that might not appear obvious because they are completed daily without much thought. Deciding who could complete these functions if a key employee is absent, if a vital supplier is unavailable or if technology is not functioning before the decision is real will lead to a more prepared workforce.

The following is a sample Risk and Vulnerability Analysis that is included in the Open for Business® Basic Trainer Series (Session 4: Developing Continuity Plans). The analysis is further explained in the Open for Business® Advanced Track, which also is available through a free download from the IBHS website. It is a good starting point for any business owner who wants to understand the eight general areas of potential threats or risks.

NATURAL	POLITICAL	HUMAN CAUSED	TECHNOLOGICAL
• Earthquake • Tornado/Wind • Hurricanes • Floods • Volcanic Eruptions • Severe Weather • Wildfire	• Strikes • Riots • Civil Disturbances • Bomb Threat • Biological Threat • Nuclear Threat • Acts of War	• Sabotage • Product Tampering • Scandal • Workplace Violence • Kidnapping/Extortion • Sexual Harassment • Fraud/Embezzlement • Terrorist Attack	• Software Failure • Hardware Failure • Power Outage • Data Corruption • Synchronization Error • Cooling System Failure • Wiring and Cables • Mechanical Systems
SECURITY	**ACCIDENTS**	**LOSS OF:**	**NEWER THREATS**
• Privacy • Viruses • Hackers • Data Theft • Counterfeiters	• Human Error • Fires/Explosions • Water Damage • Building Collapse • Environmental Contamination	• Key Employee • Senior Leader • Subject Matter Expert	• Pandemics • Water Shortage • Media Crisis • Mismanagement • Product Liability • Globalization • Virtualization

Insurance Institute for Business & Home Safety

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