FACTORY PREPAREDNESS PLANNING GUIDE

If you already have a Preparedness Plan – great! Then you can use this Guide to double check your plan to make sure it has all the components we cover.

If you do not have a formal, written Preparedness Plan, then please be advised - since every business situation is different, this document will not provide you with everything you may need, but it will put you well on your way to being prepared.

We are providing this to you in MS Word document format (.docx) so that you can use this actual document as a foundation for building your plan.

We provide additional resources throughout the document and at the end that will help make the preparedness process easier.

This Guide is divided into four sections:

1. “Basics” covers what to do for weather-related disaster planning.
2. “Modern Concerns” covers reducing risks from non-weather threats such as cyber-crime, or burglary of physical and intellectual property.
3. “Advanced Planning” addresses risk exposure from indirect sources such as your suppliers and customers.
4. The 3 Most Common Failures of Preparedness Plans

Basics

Know your Local Weather
Weather events can impact business operations all year round, so addressing your weather-related risks is the best place to start.

First, type your zip code into this site: Disaster Safety [http://www.disastersafety.org], and find your region’s weather-related issues.

For example, in:
- Hartford, Connecticut it is: Winter Storms, Floods, Hurricanes, and Wildfires.
- Los Angeles, California it is: Earthquakes, Floods, High Winds, and Wildfires.

Gather your Team
Who should be involved in disaster planning?
You want the usual suspects: upper management, Facilities staff, Human Resources, PLUS the IT department, one or more people from the production floor who have the ear of the rest of the workforce, and the building owner (if you don’t own the building).

Evaluate Risk
Set up a 1-hour meeting with your Disaster Preparedness Team. Spend a few minutes brainstorming any other weather-related events that might impact your facility.
These may include:
- Dams
- Drought
- Earthquake
- Explosion
- Fire
- Flood
- Hazardous Spill / Leak
- Heat Wave
- Hurricane
- Landslide
- Loss of Key Staff
- Loss of Utilities (Water, Electricity, Gas…)
- Nuclear Power Plants
- Pandemic
- Power Outage
- Rioting
- Snow Storm
- Terrorism
- Tornado
- Tsunami
- Volcano
- Wildfire
- Workplace Violence

Then put all weather-related events into a spreadsheet (or each on an individual Post-it note), and assess the likelihood of each of these events occurring at / to your facility. Rank them by number from Most likely / or most frequent (#1) to Least likely / or least frequent.

Next, assess the possible impact to your business from “No Effect” to “Extreme Effect”. You can use a scale from 1 to 10. For example, if a tornado hit your building, how long would your business be down? (Longer downtime = more severe = higher number)

Then multiply the Likelihood number by the Severity number for each risk event.

Put all events on a list, with greatest impactful events at the top of the list, down to least impactful at the bottom.

Take this list and build your preparedness plan around the highest-scoring event first, and then add additional components to cover the lower-scoring events. This method covers your assets from the most damaging possible events first.

Include these elements in your plan:

**COMMUNICATION**

Surveillance – How will you know when an event is coming, and who is in charge of knowing?

Set out a Leadership Structure - Who is in charge of what during emergency situations?
Communication Systems – How will you be able to ask employees to come to work, or ask them to stay home? If something happens during a shift, how will you be able to let employees’ families know that they are okay?

Set up regular reminders for employees to update their emergency contact information. Encourage employees to have an out-of-town contact they can text or call during an emergency.

Create a list of sources of external help. List who to contact and how they can help, such as:

- Local and state police
- Fire department and emergency medical services organizations
- Local government officials, emergency management office
- Local public health agency
- Local American Red Cross chapter
- National Weather Service
- Telephone, water, gas and electric companies
- Neighboring businesses
- Neighboring community organizations (schools, clubs, churches…)

**EVACUATION / TRANSPORTATION**

What do you want employees to do in the event of an evacuation?

During what event(s) is sheltering-in-place a better option?

How will you evacuate, transport and accommodate employees with disabilities, medical conditions or other special needs?

Have employees identify alternate routes to and from your facility.

**PERSONAL PREPAREDNESS**

Encourage your employees and their families to have emergency preparedness kits at work, at home and in their vehicles.

See: www.redcross.org/BeRedCrossReady

**HARDENING THE FACILITY**

Hardening is what you do to increase your facility’s physical capacity to resist damage.

What can be done to fortify the building and business to increase its post-event survival? Do you need to:

- Improve drainage around the site?
- Check that fire-suppression systems are well maintained?
- Strengthen the roof to protect against collapse from snow load?
• Secure the roof against high winds?
• Ensure all openings can be secured and made air-tight, not only to protect against burglary, but to prevent dust and fumes from getting in?
• Example: To protect your property from wind damage, install impact-resistant windows and door systems, or plywood shutters. Hire a professional to evaluate your roof to make sure it can weather a major storm.

EQUIPMENT
Obtain necessary safety equipment and supplies:

• First Aid Kits
• Safety Supplies
• Masks
• Gloves
  Automatic External Defibrillators (AEDs)
• Fire Extinguishers
• Smoke and Carbon Monoxide Alarms
Shelter-in-place Supplies
  o Water (1 gallon per person per day)
  o Food (2000 calories per person per day)
  o Means to boil water/cook and fuel
  o Bedding

TRAINING & CULTURE

You have to work the plan. Do simulated events, like the fire drills of elementary school days. Work out the bugs and faults in the systems before you need them.

For more detailed guidance, see: http://www.fema.gov/pdf/business/guide/bizindst.pdf

CONTINUITY OF OPERATIONS

Determine the minimal key business functions and the amount of staff required to carry them out.

Develop a procedure for running these minimal functions that includes contingencies for not being able to work at the factory, not having computers, not having telephones, etc…

Reach out to any business, supplier or vendor critical to the operation of the business and make arrangements regarding how you will communicate, as well as pay for and receive goods and services.

Consider business interruption insurance. It covers operating expenses like utilities, and compensates you for the income lost after a temporary closure.
Modern Concerns

Business Prep - Protect IP and IT
Did you know that over 45% of the 50 million Internet-connected, electronic devices have security protocols ranked as “poor” by the U.S. Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT)? Given that manufacturers and other large corporations are not going to give up the benefits of “big data”, information technology risks need to be managed like a core business operation.

Regular computer networks used for email are also a common access risk, and easily hacked by any number of ill-intentioned hacker groups. Access can be through brute-force attacks that overwhelm the servers, or through more covert backdoors and email phishing queries to trick employees into releasing sensitive passwords and information.

**Start here to reduce these risks:**

Know what documents / records you must have to function at the minimal level, and consider having off-site duplicates for access.

Set up off-site electronic record archiving in case all the computers at your site get destroyed, at least 100 miles from your facility. Make back-up copies of all tax, accounting, payroll and production records, and customer data, on computer hard drives, and store the records at an offsite. Have electronic versions of all important documents stored off-site; also have hard copies of these documents stored off-site. Any copies of important documents stored on-site should be in fireproof safe boxes.

Create a Code of Conduct. Define what is expected of employees and the consequences of misbehavior; then make sure all employees – new and tenured – are aware of, and sign off on it.

Conduct ‘Shred Events’. Show commitment to security by creating activities that help employees to remove old versions and destroy sensitive documents.

Have the IT Department randomly audit. Inspect document storage and electronic files of employees, share results and continuously improve the system so that it supports the employees doing the right thing.

Maintain and upgrade your software. One of the largest risks are “backdoors” that have been found in old versions of software. Patches, fixes and new versions close these access points, but, sadly, they are rarely installed.

Create tough usernames and passwords - a basic step, yet many smaller companies fail to do this. As sub-contractors to larger corporations, they become the access point to their customers. A tough password has at least 8 to 10 characters, a mix of numbers, symbols, letters, and upper and lower case.

Lock out workstations and change passwords. Change all passwords every 30 to 45 days. 65% of people use the same password across multiple accounts and fail to change it – ever!
Tools:
This website has news and trends in the IT / IP security world. Useful to know when someone finds new holes in software or a new virus comes out. 
http://www.darkreading.com/new-gaping-security-holes-found-exposing-servers/d/d-id/1140063

This site is the U.S. federal agency in charge of cyber-crimes. If you feel you have been a victim, contact them as soon as possible. 
https://ics-cert.us-cert.gov

Advanced Planning

Supply Chain Prep – Know Weaknesses and Risks

What if a disaster strikes your supplier network? Or hits the transportation network that brings you supplies? Talk to your vendors; work with them to incorporate disaster preparedness. And if they are not interested, it may be time to find another vendor.

Considering the impacts of weather, cyber-crime, and other issues upon your suppliers and supply chain transport routes is an advanced step toward preparedness. A shorter, more controllable supply chain reduces risk, and enables more control over the manufacturing process.

Discuss supply chain vulnerability with the Purchasing, Operations, Production, Quality and Sales teams. Determine what issues each group has and gather suggestions. Look into reshoring, next-shoring and shortening the supply chain by using the TCO Estimator for their reshoring calculator, and find out the cost of long-distance supply chains: 
http://www.reshorenow.org/TCO_Estimator.cfm

Going Further

Consolidating

A better move would be to expand existing manufacturing sites, and / or utilize existing manufacturing infrastructure within a short distance from the customer.

One company we know has gone back to vertically integrating the entire process in-house. By buying up and consolidating suppliers, and then moving everyone into a new larger facility (a renovated older manufacturing building) this company is poised for resilient, agile manufacturing.

The reasons to shorten the supply lines include:
• Faster delivery of product
• Reduced need for warehouse space and inventory
• Less risk of damaged goods and losses in transport
• Improved part quality
• Protection of proprietary intellectual property, or production methods
• Better trained, more highly-skilled workers
• Reduced re-work and customer complaints
• Reduced minimum order size
Be a Team Player
Help your community get prepared. Offer resources to the community leaders; educate the firefighters and first responders about your facility and what your plans are. Give back to the community upon which you might some day rely for shelter, transportation, or evacuation assistance.

Sources:
1) http://www.disastersafety.org
2) “11 Common Disaster Response Mistakes”, Agility Recovery Services, Inc. - http://www2.agilityrecovery.com

The 3 Most Common Failures of Preparedness Plans:

1) Relying upon a Single Point Solution. What happens if you are:
   - Relying upon one key person to have the emergency plan action items?
   - Using only a single means of communicating with the employees?
   - Having a single fuel type to run back-up systems?
   - For example, communication is often most difficult when disaster strikes. Make sure your key personnel have access to e-mail, texting and even landline phone systems.
   - Follow the old saying; Two-is-one, One-is-none!

2) Not adequately training ALL employees. Everyone should know what to do in the event of a disaster. Cross-training and regular practice will keep all people thinking about their roles.

Encourage your employees to use this free iPhone App for Emergency Checklists from the Insurance Information Institute, which allows you use prepared lists or create your own. https://itunes.apple.com/us/app/your-plan/id537737839?mt=8

3) Not carrying enough, or the right kind of, insurance. Schedule an annual review of your coverage with your agent, to discuss the exclusion and limits, and what new options exist for business interruption or re-building. Have a photo and a video record of your company’s assets, as well as a paper list, stored off-site. Have your disaster team calculate the cost of downtime and other expenses that arise from a disaster. Use this as a tool for making decisions on investing in equipment such as back-up power systems, flood control, alarms and communication devices.

More Tools


Here are some useful Checklists and Toolkits from FEMA: http://www.fema.gov/preparedness-checklists-toolkits