Building A Successful Business Continuity Plan

Business continuity is about more than data backup - you need a plan that prepares you to keep your business running in a range of potential disaster scenarios. Do you know what that type of plan needs to include?

Business emergencies can strike at any time whether it's a malware attack, natural disaster or pandemic. It's vital to have a plan in place to make sure your business can continue to accomplish work, maintain compliance, and keep unproductive downtime to a minimum.

Without comprehensive disaster recovery planning, you're left vulnerable to any and all emergency situations, whether it's a major meteorological event like a hurricane, common power outages, or the result of malicious or accidental employee actions. Consequences include:

- Permanent data loss as onsite copies of your data and documentation are destroyed
- Severe downtime as your business scrambles to replace destroyed hardware and get up and running again
- Major financial damages, from the cost of lost business to the cost of replacement hardware, and onsite damages

As with most initiatives, the first step is to create a workable plan. Your business' plan needs to be carefully constructed and written down for reference and review. Remember, many companies are required to maintain an Emergency Action Plan by OSHA so this can be considered part of that process.

Top 4 Priorities In Your Business Continuity Plan

Your plan should put forth policies and procedures regarding employee safety, business continuity, and contingencies that can be activated if your business' facilities are damaged.

The three main priorities of an effective Business Continuity Plan are:

- **Protecting Data:** Whether it's your on-site server, in the Cloud, or hard copy duplicates stored in the filing cabinets, you need to make sure your business' data is protected and securely backed up.
- **Protecting Property:** Natural disasters are a legitimate threat to businesses in Florida. Your plan needs to consider how best to protect your property during a disaster event.
- **Maintaining Continuity:** Whether your phone lines go down, or a pandemic keeps your team from coming into the office, you can't let disaster-related obstacles keep your business from working.
- **Mitigating Employee Risks:** Cybersecurity gimmicks -- such as "set it and forget it" firewalls and antivirus software -- fail to account for how important the user is:
  - **Accidental Deletion:** According to the 2019 Shred It Protection Report, 31% of small business owners report that human error or accidental loss by a staff member led to a data breach.
  - **Malicious Insider Threats:** Employees acting in bad faith can cause extensive damage as well. According to the 2018 Insider Threat Report, of 874 reported incidents, 191 were caused by malicious employees.

What Should Your Business Continuity Plan Include?

- **Protection Of Property:** While so much of disaster recovery these days is focused on data continuity, it's important to remember that your facilities are a resource as well, and they should be protected.
  - Make sure your windows have proper shutters or are boarded up with plywood to keep them safe from airborne debris.
  - Inspect your roof prior to each hurricane season to make sure it's in good shape.
  - Assess whether there are any aging branches or trees that could fall and cause damage during a storm. If you're unsure, have an arborist check it out for you.
  - Bring sandbags to areas that could be affected by flooding.
  - Secure heavier objects, including bookcases, shelves, filing cabinets, computers, etc.
  - Secure utilities, and raise them off the ground if necessary to avoid flood damage.
  - Relocate any fragile or valuable items to less dangerous areas, if possible.
- **Protection Of Data:** Once all your physical assets are taken care of, don't forget about your business documentation and onsite data storage:
  - Make sure you have a backup of information on important business contacts.
  - Backup documents that are not easy to reproduce or re-acquire in the event of water damage – insurance and legal contracts, tax files, etc.
  - Keep as much of your documentation as possible in waterproof containers.
  - The backup solution you use should provide both local onsite backup for quick recovery in instances of data loss, as well as offsite cloud-based backup for when your business is hit with a critical disaster. Furthermore, you can't just assume that your backups will just work when needed. You need to regularly test your backups to verify their effectiveness in the event that something goes wrong with your onsite data.
- **Checklist Of Survival Resources:** You'll want to make sure you have an inventory of all the emergency resources you'll need. These are the types of items you won't be using otherwise year-round, and so, when you do require them, you don't want to realize you've forgotten something.
  - Independently powered radio/TV
  - Three-day supply of non-perishable food for as many employees as you have onsite (including 1 gallon of water per person per day)
  - Blankets, pillows, cots, and chairs
  - First Aid supplies
  - Flashlights (and additional batteries)
  - Toolkit
  - Whistles and/or signal flares
  - Tarps, plastic bags, and duct tape
  - Cleaning supplies
  - Smoke alarms and fire extinguishers
  - Electric generator
  - A backup supply of gas and additional jerry cans
  - Cash, credit cards and ID
  - Emergency contact info

- **Remote Work Plan:** If your staff can't come into the office, how can they be expected to get their work done? It all comes down to your IT.

  Both you and your staff need the right tools in order to stay productive. If you're fighting against unintuitive software, a bad connection, or anything else tech-related, they won't be able to get much done from home. It won't be long before your business' productivity grinds to a halt.

  - Have a conversation with each employee who will be working from home and have them send information regarding their computers, smartphones, and internet connection over to you.
  - Cybersecurity will be extra important as cybercriminals will undoubtedly use the opportunity to entice unknowing victims into clicking on links or downloading information.
  - Cloud-based phone systems and collaboration tools will play a crucial role in your business - allowing your team to work from home while still taking part in conference calls, video calls, file sharing and more.
  - Make sure to provide some form of cybersecurity awareness and cloud productivity training to your staff members.
  - IT will be all the more important at this time, and as such, you'll want to make sure you have the right support services in place. A help desk support team should be available to your employees in the event of technology issues, questions or concerns.
- **Conditional Access:** The fact is that unnecessary access to sensitive data and misuse of privilege is often one of the most common ways for employees to cause damage to a business.

  Cybercriminals can trick a user with administrative privileges to download and run malware, or by elevating privileges on a compromised non-admin account, hackers regularly make use of this highly common unsafe business practice. Furthermore, malicious employees can abuse their privilege to do damage directly.

  - Limiting administrative privileges to those who actually require it. The fact is that the common business user should not require administrative privileges to do their job – whether that's for installing software, printing, using common programs, etc.
  - Protect administrative accounts. Once you've limited privileges to only a few members of the organization, make sure their accounts have the right protections in place – complex, long passwords, multi-factor authentication, configure alerts for unsuccessful log-ins, and limit administrative actions to devices that are air-gapped from unnecessary aspects of your network.
- **Identification Of Potential Risks:** By understanding the risks posed to your business -- electrical failure, region-specific weather, human error, etc. -- you can more effectively plan to avoid them. Make sure to review your local area on Google Maps to identify nearby risks, including:
  - Coastlines
  - Railroads
  - Easily flooded areas
- **Definition Of Procedures And Assigning Roles:** Determine the critical staff that will need to be on-site or on-call during an emergency. It's important to define who will be needed to keep your business running, and who should be responsible for any emergency response tasks. Remember that safety comes first and that your plan must focus on keeping your employees out of danger.

- **Coordination:** A comprehensive plan should prepare your business to coordinate with others during an emergency. How are nearby businesses going to operate? How will police, fire, and medical response be affected? These questions are best answered before the storm hits.
- **Briefing Your Employees:** Your plan should not be written and then left on a shelf. Every employee should be familiar with your procedures and plans to handle any future emergencies. Hold a meeting where your plan is reviewed, roles are assigned, and your staff can ask questions.
- **Reviewing And Updating Your Plans Annually:** Changes in your business or the community in which you operate can have a major effect on your disaster plan. Be sure to review your plan at least once a year and make any necessary revisions to keep it current and effective.

What's The Bottom Line Of Business Continuity?

Effective preparedness keeps you safe and productive, and protects your assets, simple as that.

In addition to protecting yourself and your employees, proper business continuity planning should assess your individual requirements by estimating your current data retention needs and expected growth. You can then determine what systems are critical to your business and assess what recovery mechanisms are currently in place.

Based on this comprehensive analysis, you're then able to build a preparedness plan that works best for your organization.

So, the question is: will you wait until after you get hit with a disaster to start thinking about how you'll recover? Or will you do what's right for your business, and start planning for the worst-case scenario today?

We know that you'd like to keep your business operating no matter what crisis the nation faces. With the right remote work capabilities, you can keep your staff productive and healthy. If you need help, get in touch with the BoomTech, Inc. team.