

# 13 Simple Things to Protect Your Business

*As a small or medium sized business (SMB), you have already spent time and money protecting it. You have insurance. You have locks on your doors. You use passwords in your computer applications. You are hopefully doing backups for your computer files.*

*But 50% of SMBs do not have plans in place to deal with the very bad things that can disrupt their business, things like fire, flood, hurricane, tornado, power failure, pandemic, failure of a critical supplier, death of a key executive, and so on.*

*Here are 13 simple things you can do to protect your business better. They start very simple and grow in complexity, but they are still not difficult or expensive to do.*

## 1. Talk to your staff

*Would your business last very long if your people didn't come to work? I'm guessing no. So when there's a major emergency, like a flood or a hurricane, do you know if they will come to work afterwards? Do you know if they can?*

*Your people are your most important asset. Without them, you will not respond to any disruption. So here are some questions and thoughts for you:*

- 1. Have your people prepared themselves and their families for those big civil emergencies that might happen? Every household should have its own plan for these situations. In the USA, your people can get guidance from a [FEMA sponsored website](#) (Federal Emergency Management Agency). In Canada, go to the Canadian government's [Get Prepared site](#). Other countries typically have their own sites. For example, the [Cayman Islands' "Cayman Prepared" website](#), not surprisingly, focuses heavily on hurricanes*
- 2. Can they work at a time of such a disruption? Many of your staff will have family to worry about.*
- 3. Do they understand what you might expect of them? Your planning should include an assessment of how quickly you really need to be back in operation. If you are a retail business, you will want your doors open for customers very quickly. If you are an accounting firm, you might be able to wait for 3 to 5 business days.*
- 4. Will they work? Will they work somewhere else? Your continuity plans might include an alternate work place at some distance from their normal work location. Can the employees doing critical business functions go and work there? How far away is it? Do they have transportation to get there? Do they have personal commitments to family that preclude them from traveling there to work?*
- 5. Have they agreed to work? Let them know that they are critical to the future of the business. Remember that they will be worried about their own job future if there is a serious interruption to your business.*
- 6. Have you identified competent alternates for each of your key staff? If some critical people can't work for you after the interruption, you need to know which staff can do those jobs. If you don't have competent alternates, then you will need to do some cross training.*



*So talk to your people. They will be gratified that you consider them critical to the future of your business.*

## 2. Save your data

*An old topic that's been beaten to death. But maybe not. If you are smart, you back up your computer files regularly. But where do you store the backups? You would be astonished at the number of times I have asked a client where the computer backup files are stored and get the answer "Oh, they're right here. On top of the server (or on the desk beside the server or in the filing cabinet on the other side of the server room or in the office down the hall)".*

**BIG MISTAKE!** These computer backup files are not safe. They should be moved out of the building. **Immediately.** The fire that creates smoke to damage your stock and equipment will do the same damage to your backups. The flood that drenches your office will also drench your backups. The burglar that snatches your PCs will also take your backups.

- Take your backups out of the building. Regularly. In fact, as often as it takes to make sure that your data is current enough when you have to restore it.
- Store it far enough away that it isn't damaged by the same event that damages your business.
- Make sure the backups are securely stored and accessible any time of day or night. Don't have an employee take the backups home. You might not be able to get to them when you really need them.
- From time to time, check that the backups actually contain what you want them to. Some backup programs are complex to use and you might not be backing up what you think.



Finally, think very carefully about how you do your backups. Many businesses are still using CDs, DVDs, USB sticks, and tapes. Many businesses are only doing backups monthly or even weekly.

## 3. Protect and continue your e-mail

*In a serious interruption to your business, one of the most important activities for you to continue is communication – with your staff, with your customers, with your suppliers, with your regulators, with your board. There are lots of stakeholders in your business, no matter its size, and they all want to know what's going on and how you are doing with any interruption or problem you may be having..*

*Having e-mail service, including past e-mails, contacts, calendars, is critically important to the survival for your business. Within hours of the start of the interruption, even minutes, e-mail will help you manage your interruption effectively.*

*There are a number of products and services available to help you continue your e-mail quickly and easily. (just [Google "e-mail continuity"](#) to see what I mean). But there are a couple of key features you will want to consider*

- Ability to sign on to an Internet based e-mail continuity service with your own user ID and password
- Immediate availability of your own e-mail inbox and folder contents, calendar and contacts

- *Really easy implementation. Please don't undervalue this feature. The e-mail continuity service will have to make instant copies of any e-mail activities you and your colleagues do on a regular basis before the interruption, so that nothing is lost.*

*Finally, you should consider a few issues as you figure out how to protect and continue your e-mail:*

- *Where will your e-mail, calendar and contact data be stored? You (or your regulator if you are a regulated business) might not be comfortable to have it stored in another country. You might be unhappy to have it stored too close to your business either. It might be affected by the same interruption.*
- *Can anyone else see your e-mail data? Remember this is the lifeblood of your company. It is confidential and valuable data. The e-mail data should have at least the same level of security that you have given it in your own e-mail server.*
- *How much extra workload will the preferred e-mail continuity service pile onto your e-mail server and network? Every time you send or receive an e-mail, it is copied by the e-mail continuity service onto their own servers. That means extra work for your own servers and communications lines. How much extra?*



*Go and find the service that works for you. Imagine how valuable it will be to you to do your e-mail at home even after the interruption or problem has been resolved.*

#### **4. Keep key documents safe**

*So what kind of business do you do? An important question when it comes to keeping documents safe. Because the real question is, what are your key documents?*

- *If you're an insurance broker, completed insurance application forms are key, since they are the legal document between your customer and the insurance company. They might be needed in court.*
- *If you're a lawyer, you have contracts and wills stored in your safe (hopefully in your safe!) on behalf of your clients.*
- *If you're a store owner, you probably have contracts with your suppliers and landlord. And, like any business, you have tax returns filed away.*



*So every business has key documents. We call these vital records – "vital" because it's tough to do business if you don't have them. Some vital records are mandated by law or industry regulation. You probably already know about these types of vital records. If you don't, ask your accountant and lawyer for a good start on the topic.*

*So how do you protect these vital records? Here are a couple of thoughts:*

1. *Decide what records are vital.*
2. *Check each one to see if there is a valid copy elsewhere, such as at your lawyer's office or at the other contracting party's location. This will help you decide how easily they can be re-created if it's necessary.*

3. *Make a copy of those that aren't easily re-created and store the copy safely offsite. That means secure enough and far enough away such that they won't be lost or damaged in the same event that affects your own business.*
4. *Consider purchasing a fire-proof and water-proof vault or safe. Safes have fire ratings that tell you how long the contents will last if the safe is in a fire. Ask a few questions to become comfortable about buying one. Remember, though, that this should not be your only protection for your vital records. The fire might be too savage. The safe might be damaged by something other than a fire (think sinkhole, for example). You might need to get at a vital record in your safe before the fire marshal lets you sift through the ashes that once were your business.*

## 5. Tidy up your premises

*If you've had a fire marshal in to inspect your site, you probably noticed that they are looking at a couple of key things – what can burn easily, where is it, how safe is it for your people. That means they are judging what you have lying around. If it's easily combustible, they will look closer. If it's spread all over the place, they're not going to be happy. If you are blocking (or impeding) exits, they will write you up.*

*The same goes for the inspector from the insurance company. But instead of writing you up, they will up your rate. Your insurance premiums go up and you won't be happy.*

*So, here are some quick tips:*

1. *Have a walk around your premises (including the plant or the warehouse) and have a good look around.*
  - a. *What's lying on the floor that should or could be stored away properly?*
  - b. *What could catch fire easily? Is there a better place or way to store it?*
  - c. *Is anything blocking the exits? Staff need to get out fast and easily when you are evacuating quickly. Firemen need to get in quickly when they are trying to save your business.*
2. *If you have lots of combustibles, do you have the right trash containers? Do you empty them regularly?*
3. *You might want to call up the fire department or your insurance company to have them inspect your site. They can and will offer useful guidance on how to protect your business. And I'm not just talking about fire. Floods, electrical distribution, staff health and safety – these and even more are valid topics for review. But remember, they WILL make recommendations, most of which you will have to do.*
4. *Talk to your staff about the value of tidiness. Clearly, well kept premises mean a safer work environment. Businesses with well kept premises are also more likely to survive a disastrous event such as a fire or flood. This can only be good for you and your staff.*



## 6. Review keys and safes

Don't ignore this topic if you haven't thought it through. Suppose you've had an event happen ( the hurricane, the tornado, the flood, the power outage...) and your lead manager, Fred, and you can't make it back to your office. Fred is the one that opens the office up early in the morning. You and Fred have keys to the office. Do you know who else does? Can you get hold of them? What are you going to do? If you had your keys well organized and under control, this would be easy to handle.

There are lots of other reasons to carefully track your keys:

1. When a key holder leaves your employment.
2. When a key is lost and you have to replace locks and keys.
3. When a lock stops working properly and you have to replace old keys with the new ones.
4. After a break-in, you need to replace keys.



Document who has which keys and store that list safely somewhere outside your office where you can access it when you need to. The best offsite storage place, of course, is the same place you store your business continuity plan.

And while we're at it, check out your safe. You might have a safe for petty cash, other valuables and very important documents. That safe should have a good fire rating. This is a choice that only you can make, but you should base it on some knowledge of fire ratings for safes. Here are standard ratings you might see on a safe that has been tested by Underwriters' Laboratories (UL). UL is a non-profit, independent agency that tests and rates the safety and performance of consumer products. Safes that have earned specific UL ratings will carry a UL label which designates the product's security and fire-protection ratings.

- **FR** — Fire resistant unrated insulated safe.
- **1/2 hr** — UL class 350. Protects valuables for up to 30 minutes with outside temperature of 1550 degrees.
- **1 hr** — UL class 350. Protects valuables for up to 1 hour with outside temperature of 1700 degrees.
- **1 hr+** — UL class 350. Protects valuables for up to 1 hour with an outside temperature of 1700 degrees, plus survived drop test from 30 feet.
- **2 hr** — UL class 350. Protects valuables for up to 2 hours with an outside temperature of 1850 degrees.
- **2 hr+** — UL class 350. Protects valuables for up to 2 hours with outside temperature of 1850 degrees, plus survived drop test onto rubble from 30 feet



You should note that safe fire ratings are complex and you might want to seek expert advice.

## 7. Keep key office supplies safe.

We've talked about protecting your data, e-mail and key documents. Now it's time to talk about office supplies. This is not about pens, pencils and pads of paper. You can buy those when you need them.

This is about those supplies that are unique to your business, including:

- Company letterhead
- Checkbooks
- Deposit books
- Company seals
- Pre-printed forms, such as purchase orders and order forms

Keeping them safe means storing them safely offsite. Store enough that you can carry on your critical business activities until you can reasonably replenish the office supplies. If you are using pre-printed forms and letterhead, check with your forms printer to see if they keep an emergency supply for you. Some do.



## 8. Establish digital signatures and emergency spending limits.

A scanned or digital signature is a very good idea for companies that require specific endorsements. It can be as simple as signing a piece of paper, scanning it, and trimming the image with Microsoft Paint to create a signature image file that can be added to documents as required.

Store the signature image file safely and securely offsite so that you get to it when you must. There is no guarantee that the signing officer(s) will be available when you most need them.

A handwritten signature, likely 'John Hancock', in black ink. The signature is written in a cursive style with a large, stylized 'J' and 'H'.

Also a pre-allocated and documented chain of command for standby authorizations for extraordinary expenditures is vital. You will most likely need to spend more money when you are executing your readiness plans.

## 9. Develop an emergency contact list.

You must make an emergency contact list. Then laminate lots of copies. Give them to key managers and supervisors to store at home. Revise the list regularly.

Your contact list should include contact details for:

- Staff
- Board members
- Critical suppliers
- Critical customers and clients
- Regulators



- Emergency services

The contact details should include:

- Name and company
- Phone numbers (work, home, mobile phone, alternate phones)
- E-mail addresses (work, personal)
- Smartphone PIN numbers (if they have one)
- Addresses

### **10. Know where to get definitive information about the approaching weather including hurricane, tornado, snowstorm, tsunami, flood, or cyclone.**

When something bad is coming at you, you need solid, trustworthy information to help you make decisions. Many disruptive events take time to arrive or develop before they significantly affect your company. You have days of warning for hurricanes, cyclones and floods. You have maybe a day for ice and snow storms. You have hours or even minutes for tornadoes and tsunamis.

So it makes sense to have information delivered directly to you with warnings about those impending events.

There are many Internet weather services that will send you e-mails or text messages with weather warnings for your business and home location, either directly to your e-mail or your smartphone. Check out your favorite weather service and you are likely to find their weather warning service pretty quickly.

There are other sites with information and push messaging services for other events. Here are some sites to start you off:

1. [Weather.com](http://Weather.com) - provides e-mail and mobile phone weather alerts for the USA (only).
2. [The National Terror Alert Center](http://The National Terror Alert Center) - is administered by the American Department of Homeland Security.
3. [Weather Underground Severe US Weather Map and warnings](http://Weather Underground Severe US Weather Map and warnings). Also has a mobile website for your cell phone or Blackberry browser. A linked site can also support iPhones.
4. [WeatherWatchers.ca](http://WeatherWatchers.ca) - sends you emails of weather watches and warnings as issued by Environment Canada. But watch out for the Internet Explorer bug, which is described in the site.
5. [Google Alerts](http://Google Alerts) - Sign up for email updates of the latest relevant Google results (web, news, etc.) based on your choice of query or topics.
6. [AccuWeather](http://AccuWeather) - Get daily forecast and severe weather watches and warnings emailed to you from AccuWeather.com.
7. [Continuity Central Newsflash](http://Continuity Central Newsflash) - Newsflash is an occasional email update sent out only when a significant business continuity news event happens. Continuity Central is an information resource for business continuity professionals.
8. [www.wunderground.com/tropical](http://www.wunderground.com/tropical) - Atlantic satellite map, sea surface temperature and hurricane advisory providing links to weather information around the world.
9. [www.nhc.noaa.gov](http://www.nhc.noaa.gov) - National Oceanic and Atmospheric Administration



10. Your utility company will typically have a web page and/or a notification service about current power outages
11. [www.fema.org](http://www.fema.org) – U.S. government Federal Emergency Management Agency

## 11. Develop your continuity/disaster/emergency plans.

Here's a simple chart to guide you in developing your plans. Kind of scary, isn't it? This is a bit of an eye-chart. It doesn't look easy.

However, there is a commonly accepted set of things you should do to develop a good readiness program. If you're interested, you can go and look at standards established by the International Standards Organization (ISO), the National Fire Protection Association (NFPA), or the Canadian Standards Association (CSA).



This chart illustrates 12 steps common to all the standards:

1. Starting Off – planning how you are going to develop your readiness program
2. Self Assessment – what have you already done that you can use in your readiness program, such as evacuation procedures, computer backups, and so on?
3. Risk Assessment – what are the bad things that are most likely to happen to your business? what can you do to stop them from happening? what can you do to reduce their impact?
4. Business Impact Analysis – what are the most critical activities you do regularly? when do they become critical? what do you need to get them back in operation – facilities, equipment, people, computer applications, paper records?
5. Recovery Strategies – how are you going to achieve what you decided in the Business Impact Analysis? what additional infrastructure or services do you need in place?
6. Crisis Management – who is in charge when the bad thing happens to your business? what will they do?
7. Emergency Response – what immediate response procedures do you need to protect your staff, visitors and assets, such as evacuation, bomb threats, medical emergencies, power failures, and so on? who will execute those procedures?
8. Business Continuity – What procedures will your people execute to get those critical activities back in operation as fast as you decided in the Business Impact Analysis?
9. IT Recovery – what procedures will your IT staff or service provider execute to get those critical computer applications back in operation as fast as you decided in the Business Impact Analysis?
10. Training – how will you train your people to respond as you have planned?
11. Awareness/Exercising – how and how often will you practice the procedures you have developed?
12. Keeping Current – How will you keep your new readiness program alive and well? who will own the program?

## 12. Have your continuity/disaster/emergency plans reviewed objectively.

If you have already developed a readiness program and you want to find out if it's good enough, find someone to assess the program for you. You are most likely too close to your program to do it well yourself.

This need not be a colossal exercise costing way more dollars than you want to spend. Any reputable and experienced consulting company should be able to take a very quick look at your readiness plan and summarize the gaps at a high level. We do it all the time for prospects that tell us they are in good shape.

You can also ask your external auditors to take a look. The audit firms are much more aware of the qualities of a good readiness program than they used to be. If you have an internal auditor, you might ask for an assessment.

Finally, if you really are determined to assess your readiness program yourself, you can look to the standards referenced above in "11. Develop your continuity/disaster/emergency plans". Or to keep it really simple, contact Readysmith Advisers Limited for our white paper "Are you ready? 7 challenges to assess your business continuity program easily".



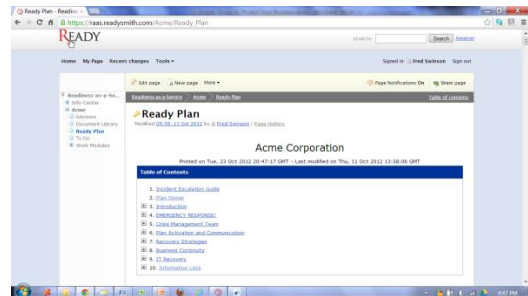
## 13. Keep it simple

Finally, in our combined years of experience in business continuity and disaster recovery, we have seen far too many examples of disjointed, siloed plans. We have seen readiness programs that produced several feet (yes, several feet on a bookshelf!) of documentation that are impossible to navigate because there is no rhyme or reason to the architecture and layout of the procedures to be executed in an emergency. Imagine standing in front of the bookcase and trying to decide which plan or document to be used next, particularly when you have just minutes to respond.

So, keep it simple. Just **one** plan for everything - hurricanes, fires, floods, pandemics, computer failures, critical supplier failure, etc.

1. One set of procedures
2. One to three teams to deal with all disruptions
3. One contact list
4. One plan owner to maintain the plan

After all, you are probably not a Fortune 100 company.



Michael Smith has spent more than 27 years consulting in Business Continuity Management. He has extensive consulting in experience in Business Continuity, Disaster Recovery, Crisis Management and Emergency Response for many of North America's largest organizations. He is President of Readysmith Advisers Limited, experts in preparing small and medium sized businesses to deal with adversity - emergencies, crises, disasters. Michael can be reached at [michael.smith@readysmith.com](mailto:michael.smith@readysmith.com). See our website at [www.readysmithadvisers.com](http://www.readysmithadvisers.com)

