

# **BULLET-PROOF YOUR BUSINESS**

**Before** you're targeted by disaster!



Flood



Fire



Hackers/Virus

Anne-Marie Moore  
**House Cleaning Pro**

## **This Special Report does NOT come with Resell Rights!**

### **Limits of Liability / Disclaimer of Warranty:**

The author and publisher of this special report and the accompanying materials have used their best efforts in preparing the material. The author and publisher make no representation or warranties with respect to the accuracy, applicability, fitness or completeness of the contents of this program. They disclaim any warranties (expressed or implied), merchantability or fitness for any particular purpose. The author and publisher shall in no event be held liable for any loss or other damages, including but not limited to special, incidental, consequential or other damages. As always, the advice of a competent legal, tax, accounting or other professional should be sought.

The author and publisher do not warrant the performance, effectiveness or applicability of any sites listed in this book. All links are for information purposes only and are not warranted for content, accuracy or any other implied or explicit purpose.

This report contains material protected under International and Federal Copyright Laws and Treaties. Any unauthorized reprint or use of this material is prohibited.

## **Giveaway Rights**

You are granted giveaway rights to this report. This means you have the rights to share this report with anyone **WITHOUT ALTERATIONS** – it must remain in its current format. You may give it away for FREE, but - you do not have the rights to sell it for profit or claim it as your own or change the copyright.

# Table of Contents

<b>1. Introduction .....</b>	<b>4</b>
<b>2. Basic Security Issues .....</b>	<b>6</b>
<b>Access to Your Business .....</b>	<b>6</b>
Access to Your Physical Business .....	6
Access to Your Website, Blog or Online Business.....	6
Passwords .....	7
Password Generators.....	9
Keystroke logging .....	9
Site Security .....	10
<b>3. Securing Your Data.....</b>	<b>11</b>
Your PC.....	11
Daily Backups .....	12
Offsite Data Storage.....	13
Online Backup Service .....	14
Backup Your Websites and Blogs .....	15
Full Backup.....	16
<b>4. Resources.....</b>	<b>17</b>
DIY Resources and Services .....	17
Complete Resources and Services Done for You.....	17
<b>5. Still Need More Help? .....</b>	<b>18</b>

## 1. Introduction

Imagine how you'd feel about having a loss prevention strategy for your business that won't cost you a dime, which could actually save your business in the case of an unforeseen disaster or systems failure. Great, right?

Well, that's exactly how you'll feel after implementing a Business Continuity Plan, otherwise known as a BCP, and a Disaster Recovery Plan, or DRP.

Unfortunately, many businesses will never implement such simple, yet effective plans, because they either 1) never understood the importance of having instituted these types of plans, or 2) never knew it was possible to do, let alone create them for free!

Allow us to show you a way for a small business to create their very own unique plans, by following these simple step-by-step instructions, which are included with this highly revealing report. Having these plans will improve the chances for small businesses to continue operations during or after significant interruptions in their workplace environment, and in their data services and storage.

Now that you can appreciate the importance of having taken these steps to safeguard your business information and property, and why you should begin the process of developing your own strategies for protecting your assets and interests, let me introduce you to my free action plans for getting started.

A Business Continuity Plan and a Disaster Recovery Plan are not the same, and although they have much in common, a BCP focuses on the process of resuming business after a natural disaster (ie: fire, flood, theft, etc.), while a DRP focuses on the storage and recovery of digital information that can be affected by any type of harmful digital event or threat (ie: viruses, hacking, etc.).

Because both a BCP and a DRP are important to your business, I have included both action plans with this breakthrough report. All you have to do is follow my guide, and take action to start protecting your business and your invaluable intellectual property now!

## 2. Basic Security Issues

Before you can establish your BCP and DRP, you should make sure you have the basic security issues established in your business. After all, if these are not well defined, **they could lead you to some very real reasons to use your plans.**

### ***Access to Your Business***

One of the issues small business owners have is controlling who has access to their business property. If you have an offline business, how do you control the keys to your office? If you service clients who provide you with access to their homes, how do you control the keys and the codes to their security system? If your business is online, how have you ensured that accesses to the websites you use are secure?

### **Access to Your Physical Business**

Key employees must have access to open the office if the owner does not perform this function. To control the keys and security codes:

- Number the keys and record who has which key and when the key was assigned and returned. Consider re-keying when employees leave, especially if they were terminated for cause.
- Assign a unique security code for each employee who has access to the security keypad. Remove the code when the employee is on vacation, sick or leaves your employment.

### **Access to Your Website, Blog or Online Business**

If you're like many businesses today, you already are, or have considered using outsourcing for your website maintenance. But beware...once someone has worked on your website, blog or any part of your online system, they have the login codes and can return at any time without you even being aware. Now, I'm not saying that all of these people are unethical, but it's up to you to secure your online presence. Why would

someone return to do you harm? Oh – I don't know, anything could happen in our new digital world. How about selling your login codes for money – that's what happens when people steal your identity. They profit from it any way they can.

Prepare the Security Checklist included with this book and track all authorized access to your online sites. That includes any services you use like your AutoResponder (eMail marketing), webhost, etc. As soon as the work is completed, change the password and document on the checklist the date when the change was made.

### **Passwords**

We have worked on computers and with software systems for a long time. Back in the early days, passwords weren't given much thought. Anything would do and it usually did. That's when computers were so new we could get away with using the names of our siblings, birthdays, and other silly codes that could easily be guessed or easily hacked.

Even when I stress the importance of using good passwords, I still discover many people don't listen. And that's when problems start...by being too lax with login ids and passwords. For login ids and passwords to work at keeping unauthorized people from accessing your account, you should keep the Security Checklist, included with this book, of who has access to which site, assign quality passwords and change them often.

Many instances of illegal and unauthorized access, and of identity theft of personal and private online accounts such as bank accounts, business websites, blogs that have been hacked, and membership sites that were compromised and totally wiped clean, could have easily been avoided with this safeguarding.

Don't let this happen to you or your business.

Here are some guidelines for keeping your accounts safe:

### **User Id**

Do not use your real name, “admin,” or “test,” as your User Id for any of your accounts. Why? Because many software programs use admin or test and these are the first User Ids hackers try. If someone has access to your full name, they will also use it to try to hack your User Ids. By using a different User Id on all your accounts, you have provided an extra level of security for your business because most hackers will concentrate on trying to break the password and won't work that hard to break the User Id.

### **Passwords**

For passwords to be secure, they must be unique and use between 12 and 20 characters, numbers and special characters. This means using just the names of your children will not make your passwords secure. That's because anyone who has your identity will probably try that first.

Just by trying the letters of the alphabet with easy words like joe, rose, flower, green, johnnydepp, etc., unscrupulous individuals can easily break your password.

The easiest and most secure way to assign a password is by using a password generator. This is software that will generate passwords on request when you give it parameters like:

- How long the password should be
- Whether or not to use letters of the alphabet
- Whether or not to use a mix of upper and lower case
- Whether or not to use numbers
- Whether or not to use special characters

The longer a password is – like 20 characters long - and that use a mix of all the above, the safer it is. Then whenever you need a password, just click on the software provided “Generate Passwords” button using the specifications that have already been set.

A word of caution – not all sites will let you use special characters. Not a problem, just go back into your password software and turn that option off. Once you have generated your password, be sure to turn special characters back on.

Now I bet you're wondering, how the heck are you going to remember all those User Ids and Passwords?

Don't even think about writing them down and keeping that information somewhere that is convenient for everyone who needs them!

### **Password Generators**

If you invest in a good password generator like [Roboform](#), it will save your login information for you, securely on your computer. Roboform also provides you with the option to access your data from any device or location. It not only saves your login codes, but it will save the login page. Therefore, all you have to do to access the site is click on the Roboform passcard name you gave it when it was saved. An example of ours would be “House Cleaning Pro.”

### **Keystroke logging**

Another reason to invest in a password generator is because it not only will go to your website when you click on the passcard name, but it will also log you in. And this will prevent [key logging software](#) from stealing your login codes when you use your keyboard. Yes, this is a not so uncommon occurrence using the Internet. [Roboform](#) will also store the identities you use to fill out forms on your computer and on the Internet.

So – just assume that anything you enter with your keyboard could be isolated and stolen – at any time.

How does this happen? Well, what you might not know about using an Internet browser is that the information is transmitted over a series of routers in the network to get to its destination. Even if you're sitting on a website entering information, the data has to travel from your Internet Service Provider (ISP) to the servers of the website you are using, no matter if the website is just down the street from you or across the globe.

That's why if you are having a problem accessing a website, you need to call your Internet Service Provider (ISP) and the first thing they will do is run a "[tracert](#)" to trace the hops along the network and the time it takes to hop from one route to the next. Any one of the hops could have a problem BEFORE your data arrives at its destination.

Now, you need to know that hackers can access the data as it travels to the destination – this is referred to as "[sniffing.](#)" Normally sniffing is used to detect problems in the network, but is also used by hackers to steal unprotected data. That's why it's important to use secured and protected networks when giving a site your personal information.

### **Site Security**

You can tell if a site is secure when it uses [HTTPS protocol](#). This creates a secure channel over an insecure network using a server certificate that is verified and trusted. Your web browser should notify you when you attempt to access a site that has invalid security certificates. It's up to you to decide to use the site or not. I recommend not using any site that has an invalid server certificate.

HTTP URLs that begin with "http://" and use port 80 by default are not secure.

HTTPS URLs that begin with "https://" and use port 443 by default are secured with a valid server certificate - secured.

### 3. Securing Your Data

The data you collect on your PC and on your website or blog is more important to your business than your business assets. That's because without your data, i.e. your customer accounts and all the information that is in your website or blog, your site information cannot be recreated once it is lost. And you cannot replace your other assets without the data to be used to rebuild your business.

#### ***Your PC***

Do you know what to do when your PC dies? This is not "if" – it's when, because they do not last very long. In fact, my first PC crashed and died less than two years after purchase. PCs that are used on a daily basis should be budgeted for replacement every 2 – 3 years.

At some point in time, everyone who owns a computer will experience the trials and tribulations of a hard drive failure. The reasons behind it vary, and could include everything from a human error to damages resulting from flood or water. Viruses can play a role as well, along with many other factors. For many years, the need to recover data that has been lost or destroyed has made data recovery such a very valuable asset.

Almost all hard drives can be recovered. Normally, if the drive is making a ticking or a scratching noise, you can use special software programs to recover the data. Sometimes, due to age or bad parts, the aperture arm in the hard drive can fail, or the platters can become damaged and lose the data that they hold. If you can't recover the information with software, you'll need to send the hard drive off and have it either rebuilt or have technicians recover your data.

Data recovery is always an option, from external hard drives that are 2 GB in size to the largest of over 300 GB, 1 TB or more of data. No matter what size external hard drive

you have, the data can generally be recovered. Keep in mind that if you've had a computer crash, you'll need to send the hard drive off to have the data recovered by technicians. Even though it may seem like your data is gone forever - the technicians that specialize in data recovery can retrieve it – at a cost to you or your business.

You can avoid the high-cost of recovering lost data simply by planning ahead.

### ***Daily Backups***

All the computers used in your business should be backed up daily to prevent data loss. The data should be written or copied to an external storage device – not your hard drive. Using an external device ensures your data is accessible when your PC ceases to function properly.

Now – what are you going to do if your external drive dies? That's right – you need dual drives in case you lose one. Having a [RAID](#) hard drive allows you to have an exact copy (or mirror image) of your PC's hard drive. When the backup runs, the data will be written to both drives. If a single hard drive on the RAID configuration fails, the RAID setup will absorb the blow and there won't be a loss of data. On the other hand, if the entire RAID configuration crashes, it will crash big time. Whenever this happens, you'll need to send it off and have technicians restore both the RAID hardware and software.

This is a good start to securing your data, but it's not nearly enough. That's because your hardware is at risk from a natural disaster and from computer theft. After all, what's going to happen to your computer and your drives if there's a fire, or a flood or power surges that fry your hardware?

The price of external drives has come way down recently from what it was just a few years ago, and you get a lot more storage space! We're not talking about GIGs – we're talking [Terabytes](#) – that's 1,000 gigabytes! Consider using a site like [amazon.com](#) to

purchase hardware because you can read online reviews from customers who have already purchased or are using the products you are interested in.

Lastly, there is one final step you need to take, to completely safeguard your data. Along with your external back up drives, storing your files to an Internet-based service is the icing on the cake.

### ***Offsite Data Storage***

Using an online service will store your data at another location separate from your business. This is what large corporations do and it's the safest way to ensure the data for your business is secure. Once you have this in place, it can be a total backup solution or it can be used in addition to your local backups.

Offsite backup companies store your data in state of the art safes, to protect them against fire, flood, and even prying eyes. This can be extremely beneficial if you're working with sensitive information.

Another great thing about offsite backups are the fact that they can be used as real storage for your data, such as historical paper files. You won't need to rely on online space, as you can easily go to the company who is storing your data and retrieve the files anytime you wish.

Another benefit of offsite backup is the fact that your data will always be protected, and you won't have to use CD or DVDs to do it. CD and DVD storage is useful for individuals, but there will be much more physical hardware needed to store most business information. This can get quite costly, but more importantly, it will use a lot of physical space to store these backup files. They can also become damaged or lost when stored in your business location, unlike an offsite backup storage.

Offsite storage is also useful if your business is in a bad area, such as a hurricane corridor. If Mother Nature has a habit of sweeping your area with floods, fires, or hurricanes, you should look into offsite backup storage immediately. They have ways to protect your information from harm, including anything Mother Nature brings. There is no need to worry about natural disasters, system failures, hard drive crashes, or data failure with offsite backup storage.

### ***Online Backup Service***

You can also use online space with most backup service companies as well. You simply upload your data to their online storage area, and then go back anytime you wish to view it. This is a very handy feature, similar to the data you have on your sites with a hosting company, only it is now separate and available to recover your main site if it is lost.

Even though you may not realize it, the data will be available anytime you need it. Online backup services are available anytime, day or night, and can be accessed anywhere you are. Most are easy to set up, and offer you very impressive security measures. They are also fast and very efficient, which is mandatory for those who need to access their files immediately.

When it comes to online backup, you can store virtually any file you need to, such as text files, digital books, contact records, pictures, music, videos and anything else you can think of. The types of storage for online backups are virtually endless, capable of storing everything you have.

Online backup services are very affordable, as low as \$4.99 USD per month. At this price, why take the chance of putting your business information at risk? Although there are many online services available, not all of them are secure and reliable. Before choosing a service, make sure it has adequate security in place to prevent data loss.

You need SSL encryption during the transfer process and additional encryption methods once the files are stored on their servers.

We use [Carbonite](#), one of the most respected services available. They have several plans for small businesses. Once you open an account, they will start a full system backup of your emails, photos, music, business contacts, and financial information. After that, files are backed up as they are changed. You have no limit on the number or files to be archived or the backup storage space you use.

Some of the other popular options available are:

- [Dropbox](#)
- [Backblaze](#)

### ***Backup Your Websites and Blogs***

Unfortunately, people think their data is safe with the web hosting company they choose. If you took the time to read the fine print in the Terms of Service, you would know they are not responsible for your data. That's because your data is stored on servers, which is just another type of computer.

Unless you have your own dedicated server, you're on a shared server with a lot of other websites. Your data is always at risk:

- From viruses and hackers
- From employees of the web host who make mistakes like everyone
- From web hosts that can and do go out of business
- From a natural disaster

Think about this – your web host is in the hurricane corridor in the US. You didn't think that was an issue for an online business when you chose them. Then you find your sites are down because your web host was the victim of a hurricane.

Or how about this one – your web hosting company disappears!

For example, one of our marketing clients was using her own hosting account, an account that she was personally responsible for maintaining. Well, one day she caught wind that this hosting company was not responding to customer inquiries and requests for issue resolutions. She also found another online business that had stated all of their sites had been lost through this same hosting service.

She immediately began research for a new system to host her sites on, but before she could complete the transfer of all her information, her sites suddenly disappeared – even the server was gone. This told me that not only was the server down, but that the web host was gone too. Yes, that's correct - the hosting company went out of business and didn't warn any of their customers. My client had no backups because they were ON her server, which was no longer accessible. What a tragedy!

Needless to say, all her websites had to be recreated, at a considerable expense I might add, and although the basic sites could still be restructured, there was considerable data that was lost forever! All her hard work and content was gone in an instant!

### **Full Backup**

To securely protect your data, businesses need to schedule a full backup on their website(s) domain nightly if they are collecting data daily. If not, then it is only necessary to schedule a full backup after changes have been made on the server.

Save your backup in the root on your server and then download it to your computer. Once it's on your computer, your PC backup will pick it up – this means it will be processed by both your backups to your external drive, and your online backup service.

Now your business is protected and you can rest well!

## 4. Resources

### ***DIY Resources and Services***

[Aweber](#) – eMail marketing services

[Amazon.com](#) – External Drives

[Carbonite](#) – Online backup service

[Dropbox](#) - Online backup service

[Backblaze](#) - Online backup service

[Roboform](#) – Secure your identity and website access on the Internet

[Website Hosting](#) – Reliable hosting with a mid-size hosting company

These resources are available in the [BCP/DRP Package](#)

BCP.pdf – Business Continuity Planning Template

DRP.pdf – Disaster Recovery Planning Template

BackupChecklist.pdf – Backup Checklist Template

SecurityChecklist.pdf – Security Checklist Template

### ***Complete Resources and Services Done for You***

Do you need help with online and specialty services for your cleaning business? [Click here](#) to open a ticket and let us know what you need. We can help!

## 5. Still Need More Help?

I'll show you how to build a house cleaning business for maximum profits using the exact process I used to break into the top tier homes in my city. Don't want to go that big? I have also taken this information and scaled it down for independent cleaners so you can make top dollar and run your service the way you want without interference from home owners. [Let's get started!](#)

If you enjoyed this Special Report, don't miss our other reports, forms and eBooks. When you need information for your house cleaning business, we're here to provide it!

View All My [Products](#) Here

View [Product Comparisons](#) Here

Join My [House Cleaning Business Mastermind](#) Group on Facebook!