Business Continuity and Resiliency for the Freelancer

By JoAnne Burek, B.Sc., MBA

Developed for the ISC/SCI Conference 2015 :: Congrès 2015

Introduction

No business is immune to disaster. Any business can expect to experience sudden unplanned incidents. To businesses, an incident is considered a disaster if it causes significant financial loss or irreparable damage to the brand. Moreover, computers are particularly vulnerable to disasters because of the range of incident types that can affect them (e.g. power disruptions and cyber-attacks). A business that relies on computers is exposed to many incidents that may result in a disaster.

We are familiar with the efforts of our governments to make us citizens prepared for emergencies. For decades, large companies have been practicing a comprehensive form of emergency preparedness, known as “Business Continuity and Resiliency Planning” (BCRP). BCRP develops, maintains, and executes plans to keep the business going in the event of an unplanned incident. BCRP and its offshoot “Disaster Recovery Planning” (DRP) are mature disciplines with proven and tested methodologies and best practices. The disciplines continue to evolve with the support of societies, standards, and certifications.

We freelancers are also subject to incidents that can expose us to financial losses and damage to our brand, i.e., our reputation. We are particularly vulnerable because of our dependency on computer technologies. Fortunately, we can use the BCRP and DRP framework to reduce our exposures. In this paper, I outline the framework and demonstrate how we can use it to build continuity and resiliency into our freelancing business.

The Business Continuity Plan

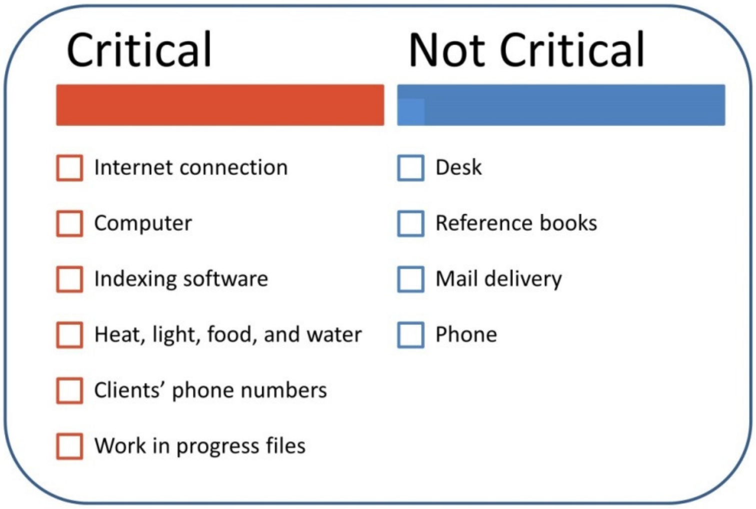
The Business Continuity Plan has the following sections:

1. **Business impact analysis** examines the goods and services of the business and estimates the maximum acceptable downtime and the impacts of disruptions.
2. **Plans, measures, and arrangements** are developed to ensure continuity, or in the event of an incident, recovery within an acceptable window of time.
3. **Readiness procedures** ensure that the plan will work. For freelancers, readiness amounts to testing the plans.
4. **Quality assurance** is concerned with keeping plans relevant and effective over time.

Business Impact Analysis

The business impact analysis for a company begins with identifying the company's goods and services and determining how long each of them can be unavailable or delayed before the company would consider it a disaster. In the case of a freelance business, it is a matter of asking yourself how long you can be unavailable before you start missing commitments or before your clients have to go elsewhere.

With this in mind, you identify your critical resources on which you are dependent. As an example, here is a list of dependencies for what I think would be a typical indexing project.



Critical

□ Internet connection
□ Computer
□ Indexing software
□ Heat, light, food, and water
□ Clients' phone numbers
□ Work in progress files

Not Critical

□ Desk
□ Reference books
□ Mail delivery
□ Phone

Figure 1 Sample critical dependencies of an indexing project

These are the resources such that if they were lost in an incident, I would not only lose revenue but I could damage my credibility with my customers.

Business impact analysis also considers financial and legal requirements. Following are some example issues:

- What is the replacement cost of the equipment I use?
- Do I have enough savings in case of an extended outage?
- Will I be in trouble with my clients if I fail to deliver?
- How will I continue to track the clients who owe me money?

Many companies also have regulatory requirements to consider in their impact analysis. For freelancers, it may be merely having our records in order (safekeeping of vital records and contracts) and staying on top of our commitments to the government (tax compliance).

Thinking about these categories will tease out all the aspects of our business that are critical to continuity.

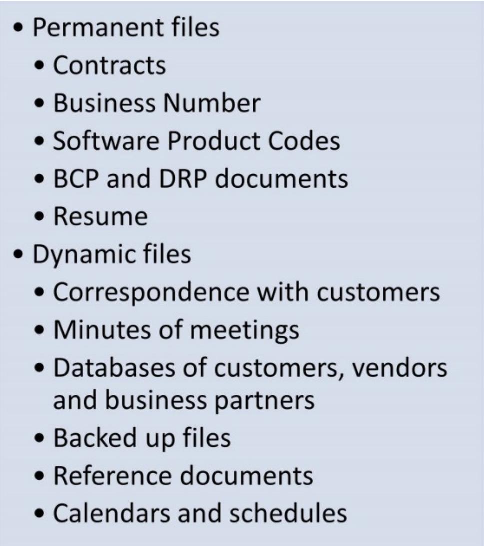
Plans, Measures, and Arrangements

The making of plans, measures, and arrangements should be done in the following order:

1. Gather your important records and create an emergency contact list
2. Implement mitigations
3. Build continuity and disaster recovery plans

1. Important records and emergency contact list

The following is a list of some of the documents that are vital to your business:



- Permanent files
  - Contracts
  - Business Number
  - Software Product Codes
  - BCP and DRP documents
  - Resume
- Dynamic files
  - Correspondence with customers
  - Minutes of meetings
  - Databases of customers, vendors and business partners
  - Backed up files
  - Reference documents
  - Calendars and schedules

Figure 2: Important documents

Separating the files into the categories of Permanent and Dynamic, as shown above, will make it easier to organize the files and to think about how you are going to protect this information.

While you are organizing your business records, why not organize your personal important records as well? The web page http://lifehacker.com/5817021/in-case-of-emergency-how-to-organize-your-important-records-in-a-master-information-kit has guidelines and a link to a template you can download from Google Docs. It will help you create a master document or a folder that you can share with your loved ones.

The emergency contact list in the business context includes the people you may need to call when you are in trouble, even if it is just to notify them. If your only record of clients' contact information is in email correspondence, now is the time to build a consolidated list of client information. Technical support numbers for your Internet Service Provider and indexing software should also be included.

2. Implement mitigations

Many disruptions can be avoided simply by implementing tools and practices. This section describes five tools you should consider for your computer setup, and presents a starting list of good practices to adopt.

A. Electronic file backup system

The number one tool is a backup system for files on your computer. If you keep your computer long enough, the hard drive will fail. The other reason to back up files is to have previous versions that you can restore from in the event of accidental deletion.

The simplest backup system can be implemented by making it a habit to periodically copy your work in progress to an external disk, a CD, or the Cloud. A more robust system includes a scheduling service that invokes backups automatically. These major operating systems have built-in schedulers:

- Apple Macintosh has Time Machine (https://support.apple.com/en-us/HT201250)
- Windows has the Backup tool (http://www.howtogeek.com/howto/1838/using-backup-and-restore-in-windows-7)

Personally, I am using "Tivoli Continuous Data Protection" as a backup scheduler, and my files are backed up daily and weekly to an external drive. This doesn't solve the problem of recovering from a disaster such as a house fire, so I am currently investigating the options for offsite backups.

Simply copying files to the Cloud is the method that many people use. Many people use Dropbox, and there are other free services that will provide the same function, such as Microsoft OneDrive, and Google Docs. The success of this method depends on how successful you are in making it a habit to use them regularly.

In my investigation of backups, I came across Crashplan (https://www.code42.com/crashplan/). This service is designed specifically for backing up home or business computers and has some nice features. The free option of the service will automatically back up your files daily to either your own external drive or to the external drive on another computer, such as in the home of a trusted friend. In fact you and your friend can both have Crashplan and back up to each other's external drives. Now you have an offsite backup without having to go to the Cloud.

But if you want to back up to the Cloud, Crashplan will do that for around $5 per month. With this paid service, backups run every minute.

You can find more information on backups at http://lifehacker.com/theres-no-excuse-for-not-backing-up-your-computer-do-1547987206.

B. Encryption software

You should be aware that when you send your files to the Cloud you are relying on the service provider's security protocol to protect against hackers. If your files are sensitive, you should encrypt (password protect) them.

Crashplan (https://www.code42.com/crashplan/) automatically encrypts files at the computer before the data is sent to the Cloud. Dropbox, on the other hand, encrypts files when they arrive at its servers. Because Dropbox has the encryption key for your files, a devious person working at Dropbox or a worker just complying with a legal request can read your data. For example, if the US Government, acting under the US Patriot Act, demanded to see your files on Dropbox's servers, Dropbox would comply and unencrypt them. But if the files had already been encrypted at your computer, the Government would have to come directly to you. Although this situation might be okay with you, it might be unacceptable to your client. In fact several Canadian companies I have worked with have refused to allow their data to be stored on US servers ever since the passing of the US Patriot Act.

To investigate how I can have my backups encrypted seamlessly before sending them to Dropbox, I tried out the following free encryption software products:

- VeraCrypt (https://veracrypt.codeplex.com) is specifically for encryption and is easy to set up but is somewhat complicated to use with Dropbox. It works with all operating systems.
- 7-Zip (http://www.7-zip.org) is technically a data compression tool which offers optional encryption. It is more complicated to set up for your Dropbox but very easy to use. It works fine in Windows, but has not been tested under a Mac.

Following are the instructions and steps I used to install and operate these products so that they work with Dropbox.

VeraCrypt encryption with Dropbox

Installation:

1. Install VeraCrypt from https://veracrypt.codeplex.com. The installation process will place an icon on your desktop.
2. Follow the VeraCrypt Beginner's Tutorial to create a VeraCrypt volume and a virtual drive. At Step 3 in the Tutorial, choose "Create an encrypted file container", at Step 4 choose "Standard VeraCrypt volume", and at Step 6, make the path name of your encrypted file container your Dropbox folder.

Note that every time you restart your system, you will have to remount the VeraCrypt virtual drive.

Operation:

The process for encrypting and backing up files to Dropbox is as follows. These instructions assume the virtual drive for VeraCrypt files is "H:"

1. Launch VeraCrypt from the desktop icon or the Windows Start menu, if it is not already running.
2. In the VeraCrypt window, select the virtual drive H and select Mount.
3. In Windows Explorer, copy the desired files to drive H. As they land in drive H, they will be automatically encrypted.
4. Dismount the virtual drive by returning to the VeraCrypt window. Select drive H and then select Dismount.
5. Launch Dropbox from the desktop icon or from the Windows Start menu. Syncing will begin immediately.

To restore a file, move or copy it from drive H. In will be unencrypted automatically.

These instructions were adapted from the web page http://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946.

7-Zip encryption with Dropbox

Installation:

1. Install 7-Zip from http://sourceforge.net/projects/sevenzip/. It is recommended that you install the program in your Dropbox folder so that you will be able to unencrypt your files from any computer.
2. Create a subfolder in your Dropbox folder to be the container for your encrypted files. This will make it easier for you to find manage your encrypted files.

Operation:

- To back up a file, launch 7-Zip File Manager from your Windows Start menu, if it is not already started. Navigate to the file to be backed up, and select Add. Be sure to add a password in order to have it encrypted. 7-Zip will create a file in the same folder with the extension ".7z". Using Windows Explorer, navigate to the ".7z" file and move it to the encryption container subfolder in your Dropbox folder.
- To unencrypt a file restored from Dropbox, launch (or return to) 7-Zip File Manager, navigate to the encryption container subfolder in your Dropbox folder, select the file, and select "Extract".

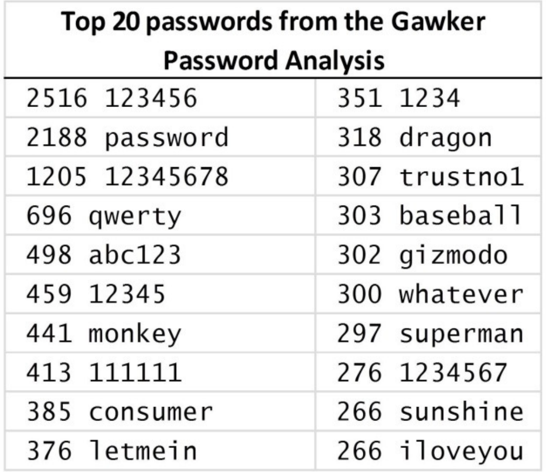
This method can get tedious if you have several files to back up. Anil Avadhani has written a set of Windows batch commands to enable you to encrypt a file and add it to Dropbox in one step using the right-click "Send to" menu. You can find the instructions at http://anilavadhani.blogspot.dk/2013/09/encypt-compress-files-and-send-to.html

C. Password manager

In 2010, Gawker Media network, which owns many popular websites, was compromised when a hacker group posted a torrent of user ids and passwords. Shortly after this event, Jon Oberheide at Duo Security Inc. wrote about it at his blog (https://www.duosecurity.com/blog/brief-analysis-of-the-gawker-password-dump):

While users may not care about an attacker having access to their Gawker account, the danger of password sharing across websites and services poses a much bigger threat. Services that lack a strong secondary authentication and host users who are sharing passwords (which, let's be honest, most users probably do) face the greatest risk. Attackers will undoubtedly be testing the cracked passwords against both personal and corporate services such as email accounts, online banking sites, VPN remote access logins.

Out of interest into the "human psychology of password selection," Duo Security took the stolen password data that was posted and used some publicly available software ("John the Ripper" at http://www.openwall.com/john/) to crack 400,000 passwords in mere hours. Then they summarized the data to find the 250 most common passwords. Here are the top twenty:



Top 20 passwords from the Gawker Password Analysis	
2516 123456	351 1234
2188 password	318 dragon
1205 12345678	307 trustno1
696 qwerty	303 baseball
498 abc123	302 gizmodo
459 12345	300 whatever
441 monkey	297 superman
413 111111	276 1234567
385 consumer	266 sunshine
376 letmein	266 iloveyou

Figure 3 Top 20 passwords

People today have many accounts with passwords. I counted 73 sites for myself, and I know I didn't get all of them. And it's hard to make up memorable passwords that are difficult to crack. Fortunately, there are many good solutions available to manage passwords for you.

A password manager is a service that secures your passwords in a vault, and for opening the vault, you only have to memorize one master password. The password manager can generate passwords that are as long and as strong you like. A password manager works offline or connected to the web. You can use it from any device, such as smartphones and tablets, and you can use it from other computers when you log in to the web service with your master password.

Following are some popular password managers. They work with any operating system:

- Lastpass at https://lastpass.com/
- Dashlane at https://www.dashlane.com/
- Keepass at http://keepass.info/
- 1Password at https://agilebits.com/

My experience is with LastPass. This service also allows me to create secure notes to keep information such as my credit card numbers and my passport as PDF attachment.

D. Anti-malware software

Viruses are just one type of malicious software. They are not very common but they make big news. More common is malware like trojans, worms, bots, backdoors, exploits, spyware, adware, and PUP (Potentially Unwanted Programs).

Today's online criminals are interested in your personal data. Besides credit card and banking details, pins and passwords, they are after your home addresses, phone numbers and even names of family members. By writing code in the form of a trojan, they can collect such identity data. In turn they can sell it to criminal organizations which can use it to steal money from your bank accounts.

Many Mac users think this doesn't apply to them because Macs don't get viruses. However, Macs do get viruses, as well as the other types of malware. Furthermore, with your Mac unprotected, you can inadvertently pass malware to your Windows friends.

There are many free products that offer basic protection. Upgrading to a paid version gives you even more protection. The following have free versions:

- Trend Micro (Windows) http://www.trendmicro.com/us/index.html
- Avast (Windows) https://www.avast.com/en-ca/index
- Bitdefender (Windows) http://www.bitdefender.ca/
- Malwarebytes (Windows) https://www.malwarebytes.org/
- Sophos (Macintosh) https://www.sophos.com/en-us/products/free-tools/sophos-antivirus-for-mac-home-edition.aspx

You can find further information at http://lifehacker.com/5807250/how-to-install-antivirus-software-for-beginners

E. Mitigating with good practices

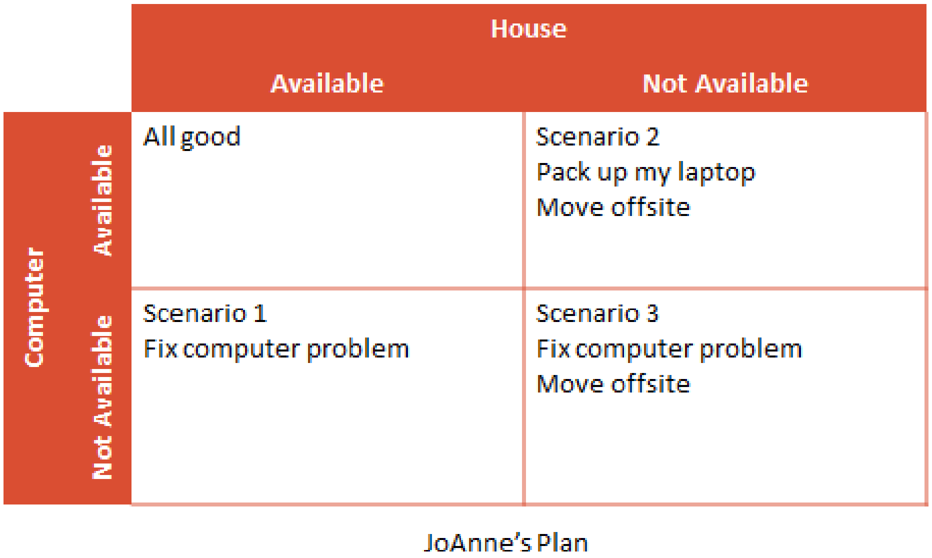
In addition to the above tools, good practices can reduce your exposure to losses due to unplanned incidents. Here are some good practices you can implement right away:

1. Perform regular backups
2. Save your work frequently
3. Keep your cellphone charged
4. Stay ahead of your work projects
5. Have a backup credit card
6. Have an emergency fund
7. Keep a list of cafés with Wi-Fi hotspots
8. Plan migrations carefully
9. Don't upgrade immediately
10. Create a recovery disk for your computer
11. Consider installing an uninterruptible power supply (UPS)

F. Disaster recovery plans

Once you have implemented all the reasonable mitigations, the task remaining is to build the plan that says how you will recover from an unavoidable incident. In this section, I explain how I approached the development of my disaster recovery plan.

No one can think of all the possible unavoidable incidents. The recommended approach is to return to the business impact analysis and review the critical resources that could become unavailable. The chart below shows my two key resources—my computer and my house. If I lose these resources, I will experience the potential disaster scenarios of “I don’t have my computer,” “I don’t have my house,” and “I don’t have my computer or my house.”



		House	
		Available	Not Available
Computer	Available	All good	Scenario 2 Pack up my laptop Move offsite
	Not Available	Scenario 1 Fix computer problem	Scenario 3 Fix computer problem Move offsite

JoAnne’s Plan

Figure 4: Disaster Recovery Critical Resources

Now I can develop my responses to these scenarios. Obviously I need the plans “Fix computer problem” and “Move offsite.”

If my computer is not functioning, there could be a number of causes. These are the causes that I think are most likely, and so I chose to address just these. It’s not hard to identify the steps that I will take to restore operations. My actual plan will go into more detail so that I am satisfied that I can read it like a checklist in a time of crisis.

Table 1: Fix Computer Problem

Cause	Steps
Computer fails to start, or has been attacked by virus	• Restore basic image from recovery disk • Restore image and data from backups
Hard drive crash	• Purchase a new hard drive • Restore basic image from recovery disk • Restore image and data from backups
Computer lost or stolen	• Order new computer • Implement plan for Working Offsite • After computer arrives, restore image and data from backups

If my house is not available I need to move offsite. I have some options from which I will choose based on the severity of the situation. I am also acknowledging to myself that if the government declares an actual disaster, I am prepared to ignore work and invoke Emergency Preparedness measures, or do whatever the authorities tell me I should do.

Table 2: Move Offsite

Scenario	Steps
I can still live in my house	Go to the nearest Wi-Fi spot
I can't live in my house	Drive to my sister's (4 hours away)
Actual disaster declared	Forget about work and invoke Emergency Preparedness instead

By thinking about unavoidable incidents from a critical resources perspective, I found solutions rather quickly for my particular circumstances. If solutions didn't present themselves right away, at least the exposures would be obvious and then I could begin to address them.

Regarding actual disasters, governments spend a lot of effort in helping citizens to be prepared. Following are some sites from government organizations:

- San Francisco SF72 http://www.sf72.org/home (particularly easy to follow)
- Alberta Emergency Management Agency http://aema.alberta.ca/documents/ema/Personal_and_Family_Preparedness.pdf
- Ontario Emergency Management http://www.emergencymanagementontario.ca/english/beprepared/beprepared.html
- Emergency Management BC http://www.embc.gov.bc.ca/em/hazard_preparedness/Personal_Safety.html

Readiness Procedures

You have created your plans, implemented your measures, and made your arrangements. How do you know they will work?

Large businesses determine their readiness by conducting tests. Because they have complex interdependencies between teams and roles, they often break it down and run table-top exercises, which use a small team and address specific areas of a business. Or they may run large-scale complex exercises which involve many people and may include evacuations.

The scope of your testing is up to you. First determine the objective of your test, which may be along the lines of recovering from a specific type of incident, for example:

- Confirm that you can restore a file from backup, or
- Confirm that you can install a new hard drive and restore everything on it.

For the second test, you can rehearse the task without actually installing a new hard drive, by walking through the order process as far as you can, and actually phoning the numbers of any technical support people that you may need to call.

Regardless of how much or little you choose to test, it is important to test it deeply, in other words, to go as far as you can to validate it. That will make it a more effective test. In testing, keep notes about what you tested, what were the results, and how long it took to do the test.

Quality Assurance

The final section of your business continuity and resiliency planning is to maintain the validity and effectiveness of your plan. There are two situations when you need to update the plan:

1. When there is a change to your environment, for example, getting a new computer, using a new service, adding new software, and
2. When there is a change to a threat.

In addition you should confirm the plan by testing on a scheduled basis. Businesses that are conscientious about this do it annually at a minimum. An important component of business continuity planning is identifying when the plan will be tested.

Conclusion

In his book “The Black Swan”, Nassim Nicholas Taleb defines a black swan event as something unpredictable by virtue of it never having happened before. His famous example is the 9/11 attack, which was so unexpected, it could never have been planned for. And because black swan events are unexpected, the impact can be extreme.

He states that “the probability of very rare events are not computable; the effect of an event on us is considerably easier to ascertain (the rarer the event, the fuzzier the odds). We can have a clear idea of an event, even if we do not know how likely it is to occur. I don’t know the odds of an earthquake, but I can imagine how San Francisco might be affected by one.” He goes on to say that how we mitigate against these rare events is by being prepared for consequences.

In this paper, we walked through the process that large companies use to be prepared for consequences. We explored how to identify the critical resources by conducting a business impact analysis. We saw that the easiest and most immediate thing you can do is gather your important records and make an emergency contact list. We explored the latest tools you should have to mitigate against common known threats, such as hardware failures, hackers, and malicious software, and we identified some best practices to adopt. We touched on the building of disaster recovery plans. We finished our preparation for bad consequences with the introduction of testing and maintenance of business continuity planning.

I hope this paper gives you some ideas you can implement right away, and that you can use this practical framework to imbed business continuity and resiliency into your freelance business on an ongoing basis.

References

The following websites provided information and inspiration for this paper:

- http://disasterrecoveryforum.com/
- http://blog.sungardas.com/
- http://www.continuitycentral.com/
- http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-eng.aspx ("A Guide to Business Continuity Planning" Public Safety Canada)