i

Abstract

Yay, you are in business! You've created your company, you have your occupational license, your office and storefront set up, vendors, product lines, and best of all, customers!

But are you ready to open? What happens when things go wrong? Let's face it, adversity comes in many flavors. Sure, emergencies like a fire, and disasters like a hurricane are adverse, but there are more adversities to consider. A storm, or a crime, your internet goes down, or even something like if your suppliers stop supplying.

So what happens during these adverse conditions? What are your real risks, and how will you protect your business – and your customers – from the risks? Good resiliency planning will keep your business operating when things just don't go right.

This paper helps you explore your exposure to and remedies for adversity. You don't want to be in a position of trying to figure out what to do during a crisis. As some of us have heard through the years, *prior planning prevents poor performance*. Will this planning make you 100% safe from adverse conditions? Of course not. What it will do, though, is help you understand the risks your company faces, and help you get through the situations.

In this paper, we'll focus on business continuity and resiliency planning as it relates to your product, to your business process, and to retaining your customers. We'll look at snippets of what winds up being important to different kinds of businesses, including an Ice Cream Shop, a Home Health Agency, a roofing company, and a Restaurant. Although the content is appropriate for all businesses, the intended audience is the small business. We'll avoid going through the purely educational process of defining Business Continuity and Disaster Recovery; instead, we'll look at practical, real life examples of what you need to consider when it comes to protecting the interest of your company.

Title Business Continuity and Disaster Recovery Planning for the Small Business

Subject Small Business Continuity Planning

Audience This paper is written for the small business owner. This paper is intended to provoke the reader to consider resilience management for their particular industry.

Last printed 05/20/13

Revision history

Date	Rev	Description
03/13/13	1	Initial release of the paper, audience is for Small Business Owners and those just starting a small business.
03/14/13	1.1	Added Revision History, corrected images, and updated table of contents
05/20/13	1.2	Corrected text, added example, added artwork

Table of Contents

1 Introduction to Business Continuity

When it comes to starting your business, there is no one "right type" of plan. There are business development plans, financial and budget plans, marketing plans, and recycling plans to name just a few. These are all great plans, and very important to any business. But let's face it, some are more important than others.

And when it comes to protecting your business from adversity, there is truly no one "right type" of plan. These are the plans that you hope to never use, plans that are only important when things just go wrong. But equally so, these plans are important – to both your customers, and to your business interest. Take these examples,

- What happens if your building burns to the ground? Are you going to set up shop at a temporary facility, or will you cancel all pending orders? How long will it take to recover? And how many pending orders will you lose? How will this affect your customers? To manage this risk, have you installed sprinkler systems? Or a fire alarm that automatically calls the fire department when things go wrong?
- How about a hurricane warning? Do you send your workers home? How is your customer base affected by hurricane warnings? If you are selling water, you stay in business since everyone and their brother will be looking to buy water! But how about if you are an Ice Cream shop? Do you expect to get much business while everyone is scurrying around trying to board up their windows? How about if you are a licensed Home Health Agency? You may have government regulatory demands in place that force you to stay open, or maybe even force you to move all of your patients to a safe house for continued care.
- How about a tsunami that happens quite quickly? You may say, "Oh, but I'm in Florida, we don't have tsunamis." This is true, you don't. However, your suppliers may by affected, and if your suppliers are affected, you are affected. Take for example the 2011 earthquake and tsunami that affected Japanese LCD and semiconductor manufacturers, thereby disrupting the worldwide supply of these components.[1] [2]

Certainly, you may not know at this moment what you will do in these situations. It will likely depend on many factors, such as what is your business backlog of orders. However, it is never a bad idea to have a plan, and planning may even clear up some of these unknowns.

As a reminder, plans are just that, just plans. As Winston Churchill is quoted, "Plans are of little importance, but planning is essential." Yeah, maybe. Then Mike Tyson tells us, "Everyone has a plan until they get punched in the face." What do we take away from all this? Have a plan, but don't be a slave to it. Be comfortable in changing the plans as necessary. These types of plans are truly living documents. You already know your

1 "Computers, Electronics and Autos Hit by Japan's Tsunami", MAR 24, 2011, http://news.discovery.com/tech/computers-electronics-and-autos-hit-by-japans-tsunami-110324.htm

2 "The Impact of Japan's Earthquake on Tianma's LCD Business and our Countermeasures", http://tianma-europe.com/downloads/tianma-letter-to-customers-on-311-earthquake-e.pdf

business. As you get to know more about risks, your risks plans will become more mature. In these first phases, you may or may not even document the plan – the goal is to understand your risks.

Let's look at what we are trying to achieve here and set some expectations. This is not a Business Continuity Training document. It is intended to look at real life threats and impacts to your small business. When we think Business Continuity, we should be thinking about, "what are the threats and risks to my business when it comes to completing my mission." That is, what adverse situations might happen that will negatively impact completing your business goals. In this document, we'll be looking at ways to reduce the impact of those adverse situations. We will be examining real life scenarios for real life companies, including a retail ice cream shop, a home health agency, and a restaurant.

This paper will consist of the following sections. First, we will lay out objectives or principles of the risk plan that we are writing. Next, we will brainstorm business continuity threats and risk impacts to your business, taking note of all conceivable risks (some of these will be unreasonable, and we can eventually discard them as unreasonable). Then, we will outline how to document the business continuity risks and associated mitigation. Finally, we will detail some of the risks and mitigation steps required to successfully keep your business running. Along with this, we will outline how much it is going to cost to implement the risk mitigation. We'll end with some concluding remarks and way forward for developing a more comprehensive business continuity plan.

2 Objectives and principles of Small Business Continuity Planning

In this paper we are going to talk about Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP). But what exactly is BCP, and what is DRP? First of all, BC and DR are not the same, they are not synonyms for one another. In short, the DR has a much more narrow scope than the BC; in fact, the DR is often solely a function of the IT department and focused solely on data processing, while BC has a larger scope that addresses the business at large.[3] [4] You can best think of the Business Continuity Plan as the "umbrella policy" that makes sure the business continues, and the Disaster Recovery Plan is a supportive plan, a piece of the puzzle to make sure that the Business Continuity Plan works as expected. With all that said, BC and DR are closely related, and certainly in layman speech, the two are often used as synonyms.

What are we planning to achieve with planning for adversity? The objectives and principles of the Business Continuity Planning include:

- To identify as many risks to the business as possible. Realize, you don't have to document a corrective plan or mitigation plan for every risk that is identified, so be liberal in writing your risks down.
- To create reasonable risk aversion plans that can be budgeted accordingly. Every planned mitigation will likely need some form of financial backing.
- To make the plan simple, short, practical, and achievable. Simple, so that they can be executed without having to rethink the steps; short, so that they can be executed in a reasonable amount of time; practical, since an impractical plan will not help; and achievable, since if the plan cannot be completed the plan will not succeed in helping to mitigate the risk.
- To make the plan testable. Sure, it is great to have an idea of what to do in case of a crisis, but it is even better to see how that plan works out in real life.
- To make the plan extensible and easy to change as new business needs are discovered and technology evolves. Like we've said, plan, plan, plan, but don't be a slave to it.

3 According to the SANS Institute1, a properly developed BCP is actually composed of the following five different assurance plans: Business Resumption Plan, Occupant Emergency Plan, Continuity of Operations Plan, Incident Management Plan, Disaster Recovery Plan. "The Disaster Recovery Plan," SANS Institute InfoSec Reading Room, Chad Bahan, June 2003, GSEC Practical Assignment version 1.4b. http://www.sans.org/reading_room/whitepapers/recovery/disaster-recovery-plan_1164

4 "Disaster recovery vs Business continuity", Dejan Kosutic, November 04, 2010, ISO 27001 &ISO 22301, http://blog.iso27001standard.com/2010/11/04/disaster-recovery-vs-business-continuity/

3 A little background about risks

Before we get too deep in brainstorming the risks, let's describe the various ways to manage a risk. If you better understand that you have options when it comes to risks, you may be more comfortable with the risk brainstorming cycle.

3.1 Risk ACAT

Risks in themselves are not "bad". In fact, risks can create opportunities – some businesses actually cater to helping people manage their risks, like portable air conditioning services are there to help people in crisis, where their primary air conditioning system has failed.

But risks can be bad, especially if they are not managed correctly. How can we reduce the likelihood or the impact of a risk? There are basically four ways to manage risk,[5] and a few more we'll discuss. Makes this pretty simple, no? We'll look at each of these options in the order that you should be looking at them.

3.1.1 Avoid, eliminate, or withdraw from the source of the risk

First, you can avoid the risk altogether, that is, eliminate them completely. Now that sounds great, right? Avoidance is extreme mitigation! But risk avoidance is likely not practical in most situations. Let's look at a few situations.

Let's say you are a software shop. You'd like to add a new function to your software that includes automatic electronic data transfer to a bank. You realize this is a risky function, since it will have regulatory impact. In this case, you can avoid the risk by not implementing the feature. There is a drawback, though, and that is that you may lose sales because the feature is not present. Is this reasonable? Maybe.

Take another example, say you own a hair salon. You realize there is a risk that someone may get cut with a pair of scissors, and in fact the insurance company has identified the hazard and offered a significant discount if you do not use scissors in your practice. Great, to avoid that risk, get rid of all the scissors! But is this reasonable? By avoiding the risk, you are also avoiding any hair cut engagements that require scissors. Sure, you can still do clipper cuts and razor shaves, but you cannot layer hair with scissors. Does this sound reasonable? It may be fine if you are on a military base and only cut men's hair in a strict military style. It may not be so fine if you also cut hair for the wives of the servicemen.

3.1.2 Control, reduce, optimize, or mitigate

Second, you can reduce or "control" the risk.

Controlling the risk is actually two exercises in one. The first is to control the likeliness of a risk, that is, reduce the likeliness that the risk will occur. For example, say our software shop has been hired to create a feature rich point of sale system. We may mitigate the risk of not meeting the customer's feature list by increasing the schedule or by adding additional engineers to the staff. An option to reduce the likeliness of not meeting the customer's expectation is to use a spiral, agile, or incremental release schedule in lieu of a waterfall development lifecycle so the customer is able to see early on what they will be receiving in the end.

---

5 The US DoD categorizes the four options as Avoid, Control, Accept, or Transfer (ACAT).

The second is to control the impact of the risk, that is, reduce the negative impact to your business. You can install fire suppression equipment to reduce the impact of the fire. You can install lightning rods to reduce the impact on the building and it's contents from the damaging effects of lightning strikes. You can install redundant or high availability computer equipment to reduce the impact of technology failure that would otherwise negatively affect your business (systems remain operational through a failure).

A part of mitigation is monitoring. Say for example you are a roofing contractor and have a firm fixed price contract to replace a roof. Since this is FFP, you are responsible if material costs increase – but there is also an opportunity to make more money if you purchase the goods at a better price. You may decide to monitor the selling price until the kickoff. If the price goes up to some pain threshold and you believe further price increases are coming, you may purchase the goods early. If on the other hand, prices continue to erode, you may wish to continue to monitor until you absolutely need the material.

3.1.3 Transfer to another party

Third, you can share, or "transfer" the risk. Transfer of risk is actually quite common. Most of us have car insurance. Car insurance is transferring the financial risk of an accident to a third party.

There are also other forms of insurance. Say you are hiring a small computer and Information Technology shop to do a highly important deployment. You may wish to purchase "key man" insurance to transfer some of the risks associated with hiring this shop, just in case the key man dies during the deployment. Another common form of insurance to transfer or share risks is E&O or Errors and Omissions insurance. This form of professional indemnity insurance or professional liability insurance helps to protect you in defending against negligence claims.

3.1.4 Accept, or retain

If all other options are too costly, too disruptive, or otherwise unacceptable, you can retain, or "accept" the risk. This is kind of like "self insurance". Accepting a risk is completely viable where the cost of other mitigation options is too costly. Take for example insurance policies that normally do not cover acts of war. If your business is destroyed by an act of war, you are by default self insured, and you have accepted the risk.

Say you are part of a Business Warehouse Cooperative. You realize there is a risk that a hurricane could hit. It is impossible to avoid this risk, since you happen to live on the Gulf Coast. You can mitigate the risk by installing hurricane windows and shutters, and you have off site backups and online cloud computing resources to protect your data. But there is still residual risk, you could lose your building, and you could lose your customers. You look into hurricane insurance and Business Interruption Insurance, and you believe the likeliness of occurrence is less than the cost of insurance. In this case, you self insure, and after all the mitigation, you retain the residual risks associated with a hurricane strike.

3.1.5 Another option: Exploit

Exploiting a risk is an interesting idea. If you are a Home Health Agency, and you see a significant risk with HIPAA, you may create a new business focused on helping Home Health Agencies with HIPAA compliance.

3.2 Recovery objectives and other important concepts

There are a few critical objectives to keep in mind when recovering from an adverse event[6] [7] The Recovery Time Objective (RTO) is the maximum amount of time that a recovery from the adverse situation should take. That is, if your building burns to the ground, how long can the business survive before you are fully operational and continuing business somewhere else? As you may expect, reducing the RTO increases the cost of doing business. If you want to be fully operational with zero down time, then you have to have a hot backup site ready to take over all business – a task that is very expensive. If on the other hand you have no secondary building, no on call staff, and no off site machinery, your RTO is going to be longer than the hot backup scenario.

The Recovery Point Objective (RPO) is basically "how much data can I lose during an adverse event". The RPO has an impact on how often you make backups of your computers and of all your data. That includes your check register (which would be lost in a fire), your mailroom (packages that are set for shipment), and your computer system. Say you run a hotel. How many reservations can you lose before causing a real impact to your business? Your answer may be zero, because you are a very high end hotel that caters to very high end customers. If you lost one customer's transaction through an accident, you may lose quite a bit more in reputation. In this case, you can invest more heavily in IT duplication, including off site replication, to reduce your RPO during adverse events.

The Minimum Business Continuity Objective (MBCO) is the minimum acceptable level of service under which the business can operate. That is, what minimum services are required during a disruption in order for your business to continue? The higher or more comprehensive the MBCO, the more costly disaster preparedness will be.

The Residual Risk is the risk that is "left over" aver all the brainstorming, documenting, transferring, and mitigating. Let's face it. Even after thoroughly applying the risk management guidelines, you will still have risk. Some will be documented, and some will not be documented, and some will not even be known – that is, you simply will not know what they are until they unfortunately strike.

6 "What is the difference between Recovery Time Objective (RTO) and Recovery Point Objective (RPO)?", ISO27001 Standard, Dejan Kosutic, January 30, 2012. http://blog.iso27001standard.com/2012/01/30/what-is-the-difference-between-recovery-time-objective-rto-and-recovery-point-objective-rpo/

7 "Minimum Business Continuity Objective (MBCO)", BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR).

4 Brainstorming threats and risks

To put the record straight, you know your business better than anyone else. But do you know your risks? Maybe some, and maybe not. Odds are you will not be able to identify all risks and threats to your organization. The objective of this BC planning is awareness – what identifiable things can happen that may have a detrimental effect on your business, and how can you best manage those threats?

When reflecting on your business, be especially sensitive to Single Points of Failure (or SPOFs). Sometimes SPOFs can be avoided (like, having multiple suppliers); while at other times, SPOFs are more costly to avoid (like, a single retail location). Again, awareness is key.

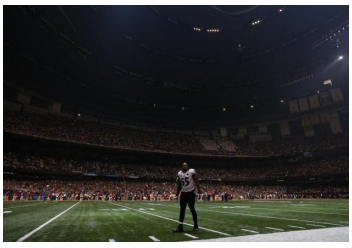
In an academic Business Continuity Plan, we'd start with internal and external threats,[8] and build towards the impact or risk those threats imply on one's business, then mitigate those risks down to acceptable Minimum Business Continuity Objectives. Finally, we would test those plans in action, and gain experience on how to fine tune the plan for success during a crisis.

We are going to work this plan a little differently. In this section we'll reflect on your business at large, and systematically look at some areas that may negatively impact your business.[9] Instead of looking at threats first[10], we are going to look at your operation, identify your risks, and apply risk management techniques to reduce your business's exposure to those risks.

4.1 Technology & utility risks

Nearly all businesses run on technology. We use technology for customer contact, schedule planning, manufacturing, order taking, placing orders with our vendors, and billing just to name a few. Without a computer, a phone, lights, and water, our business ceases.

4.1.1 Power outage



Power interruptions are the most common form of Business Risk. What happens if the power goes out? You've likely lost your computer and customer contact information, you may not be able to create shipping labels, your Point of Sale system and credit card validation system will go off line, and you won't be able to generate customer bills. Think it won't happen to you? It happened during the Super Bowl, and it could happen to

8 Per the BCM Institute, threats are categorized into Meteorological (natural), Social (man-made), Technological (man-made), Medical, and Geographical (Natural). Please see Appendix A for more information

9 Just for a little clarification, "A Threat is an indication or warning of probable man-made or natural situation that can cause disruption to an organization's operations or services" while "Risk is the potential loss exposure due to a threat; which causes a disruption to business operations, and preventing them from achieving the Minimum Business Continuity Objective (MBCO)", from BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR).

10 This plan is not reinventing a wheel. For example, "Risk Assessment as Part of Business Continuity Planning is Overrated", July 12, 2012, Frank Trovato, infoTech Research Group identifies a method similar to the one in this paper. http://blog.infotech.com/research/risk-assessment-as-part-of-business-continuity-planning-is-overrated/

you, too.[11]

Let's say you own a restaurant. If the power goes out, what do you do? Your gas grills remain operational, and you've already committed to have your staff on site. You have an inventory of fresh bread and meats. And best of all (or worst of all!), you have customers with real money at your door. You may or may not know how long the outage will last, you may not even have any idea. Have you mitigated this risk by purchasing a generator? Do you pull out the candles and offer Candlelight dining service until the outage is corrected? If you send your customers away, you may lose your customers. If you offer your customers a 50% off discount for their troubles and Candlelight dining service, you may wind up putting everyone at risk in case of a fire. If you chose to send all of your staff home and turn away your customers, then the lights come back on ten minutes later, you may be very disappointed in your decision.

Okay, if it is only a power outage and everything else is operational, you've decided that you will remain in business. But what does it take to stay in business? Make sure to have sufficient candles or other light sources on hand. Also confirm that the Fire Marshall does not cry foul. Show your plan to him during the next annual review. Make sure you have an alternate way to collect credit card transactions, maybe a mobile application on a backup cell phone.[12] Make sure you over staff since your employees will have to do more work. Because of the risks with the credit card rejection, you might even want to assign one person to do all the credit cards. Maybe have a plan where you can make your bar available and offer complementary finger foods while people are waiting. Have a plan that after the outage you are able to reconcile all of the receipts into your billing system. Of course, you will have to budget appropriately to mitigate these risks – for example, buying ice is going to be a lot more expensive than making it yourself. With this in mind, you'll have to evaluate the increased cost of the "lights out" plate, the cost of your reputation, and the cost of employees before you can make a reasonable assessment of whether to stay open or not. If you do stay open, The most important part will be to make sure your employees understand what you are doing, and understand what they are doing. Chaos breeds even more risks, so you don't want that.

4.1.2 Computer failure

What do you do if your computer fails? Or if you get hacked with a virus that takes your system down? How about if your printer fails? Can you quickly replace your Point of Sale printer with an off the shelf device from the local office supply store if it breaks? Would you need to call an IT Company to help you get back in business quickly? Have you retained them, paying them a small amount of money to keep them "on call", or are you going to just walk through the Yellow Pages and find the next available computer shop?

If you are a small retail store, your computer system will include inventory, point of sale, customer tracking, and accounting to name a few. What happens if the point of sale computer fails? Do you have to stop all sales? If you've purchased a specialized point of sale system over the internet from China that took three weeks to arrive, what are you going to do in the interim while you are having a

11 "Super Bowl blackout caused by device installed to prevent power outage", http://www.cbsnews.com/8301-400_162-57568360/super-bowl-blackout-caused-by-device-installed-to-prevent-power-outage/

12 There are a number of mobile credit card transaction companies, including Intuit (http://gopayment.com/) and PayPalHere (https://www.paypal.com/webapps/mpp/credit-card-reader)

new one sent?

Ways to mitigate against the impact of computer failures, including backups, RAID[13], secondary on site systems, off site systems, and Cloud computing to name a few. Also, investing in a UPS and (if you are a manufacturing shop) purchasing environmentally hardened computers[14] will help to reduce the likeliness of a failure in the first place.

4.1.3 Internet or network connection failure

Sometimes an internet failure is just as bad as a computer failure, but the business impact may be very different depending on your type of business. An easy Internet failure mitigation is simply to have a second internet connection, such as a prepaid wireless internet account that you will use only for the Point of Sale system.[15] In mitigating, you can purchase the device and test the service to confirm it works for your application, then just keep it handy in case you need it.

Do you have a Point of Sale contract with your credit card vendor that says every card transaction must be verified through the internet? Is there a phone based backup service that you can call in case of internet outage? Is it more costly to "call in" the credit card? Would calling in the credit card verification be unreasonably slow at the cash register?

4.1.4 Phone system

What is impacted if your phone system fails? You cannot call suppliers, customers, nor staff. You also cannot call 911 in an emergency. Your customers cannot reach you. Do you purchase an emergency use cell phone? Do you augment all of your staff with cell phones?

To control the risk against a phone system failure, you may preemptively select a provider that allows you to forward calls to another system your system is offline. Say you have a VOIP system. If your internet goes down, so does your phone system. Can you use a wireless internet provider as a backup? Maybe, be sure to test the service before relying on it, though.[16]

4.1.5 Water or sewer system

What happens if your city water or sewer fails? It really depends on the type of business you are running. If you are running a restaurant, bathrooms will be out of service, employees will not be able to wash their hands, sewer backup might introduce unacceptable odors, you won't be able to provide drinking water to your customers, you won't be able to cook any food that requires water, and you won't be able to clean up.

How can you manage these failures? For bathrooms, you might see about making an agreement with your neighbor for this kind of failure. For fresh water supply, you might send one of your employees to

13 RAID, or Redundant Array of Independent Disks, is a storage technology that helps to eliminate a hard drive as a single point of failure. The technology red

14 "A rugged computer is ... specifically designed to reliably operate in harsh usage environments and conditions, such as strong vibrations, extreme temperatures and wet or dusty conditions", http://en.wikipedia.org/wiki/Rugged_computer

15 Integrating a dual internet connection may require professional assistance and is beyond the scope of this document.

16 Wireless internet normally has higher latency than is acceptable for VOIP (contrast latency in ms with speed in kbps).

the closest store to buy water at retail prices – which will be very expensive. You will also need a way to dump waste water. If you have a sewer drop outside your back door, that could work in a pinch, but make sure you contact your Certificate of Use and Occupancy office for zoning before doing so.

4.2 Supply chain risks

The Supply Chain is particularly interesting when it comes to risk analysis and mitigation.[17] You likely do not have a lot of control on the supplier as a small business.

The loss of a supplier may have devastating and lasting impact on your company. Take for example a single lightning bolt that caused a small fire at the Philips Electronics factory in Albuquerque, New Mexico in 2000. At the time, two of the largest companies impacted included mobile phone giants Nokia and Ericsson.

In the case of this short lived fire that lasted only ten minutes before being extinguished by automatic on-site fire suppression equipment, the supply chain providing semiconductors for new an innovative phones was interrupted for months. Nokia was ready for the disruption, took appropriate mitigation steps, and managed to increase their market share in the aftermath. However, Ericsson was not prepared and lost significant ground in the mobile space. [18] [19]

So, what is important to consider when it comes to the supply chain? In a general sense, the supply chain includes the manufacturer, the distributor, and the delivery method.

4.2.1 The delivery method

It is likely very easy to replace UPS with USPS or FedEx, or sometimes bicycle messenger or even truck delivery, although each method may increase the cost of goods delivered. The increased cost of goods may have a detrimental effect on your company's bottom line, and it may not even be practical to entertain this loss of profit in a long term outage. What could happen with the delivery method? The company may go out of business, there may be a labor strike, or there may be government sanctions against an international shipper. Or there may be short term disruptions, such as delayed delivery during holidays. How might you combat these short term disruptions? Maybe use more expensive guaranteed two day delivery for essential packages?

Here's a delivery risk. Say you own an ice cream shop, and the ice cream is delivered FOB[20] the distributor. You've sent your freezer truck to get the ice cream, and on the way back your driver is involved in an accident that disables the freezer. Do you rent a freezer truck, go get the ice cream, and deliver it safely? Have you mitigated this risk by purchasing a second freezer truck, or a partial share in a freezer truck that you share with another company? Or do you transfer the risk to an Insurance Agency, paying them a fee every month to "insure" your goods transferred, and the ensuing loss of revenue? Sometimes transferring your risks to another agency is reasonable, at other times self insurance is more reasonable. But both scenarios should be reviewed.

Now say your ice cream truck is disabled for a few weeks while it is being repaired. Have you

17 "How to avoid channel failure", QDI Strategies, Steven D. Bassill, http://www.qdistrategies.com/whitepapers/HowToAvoidChannelFailure.pdf

18 "The Disaster Tab," One World, One Future, One School. By Lawrence Lanahan. "Natural disasters are unpredictable. Can businesses make them survivable?" http://carey.jhu.edu/one/2011/fall/the-disaster-tab/

19 "The Fire That Changed an Industry: A Case Study on Thriving in a Networked World," by Amit S. Mukherjee, Financial Times Press, http://www.ftpress.com/articles/article.aspx?p=1244469

20 Incoterm, Free On Board,

accepted this risk with a bank account or line of credit holding enough money to buy another ice cream truck, then sell your old one when it is repaired? Or will you mitigate the risk through rental trucks, or trucks for hire, that you can use in such an emergency as this one? Or have you accepted the risk with the thought of simply going out of business for a few weeks? If this accident happened in November and your Ice Cream shop is in Cape Cod, you were already going to close for the season. In this case, it may be appropriate to consider a seasonal risk plan.

4.2.2 The distributor, supplier, or agent

The particular distributor you use may be easy to replace, or maybe not, depending on the type of distribution system the manufacturers use since some manufacturers use exclusive arrangements with their master distributors. If at all practical, it is important to have secondary distribution channels in place in case of a disruption.

For example, say you are a computer support shop. In general, you may buy from several different distributors since each distributor might be better priced for different items. If your primary source of memory is out of stock, you will likely be able to buy memory from some other source. It might get really expensive, but buying from an alternative distributor is an alternative.

4.2.3 The manufacturer

The manufacturer may or may not be easy to replace, especially if the components are custom or highly specialized.

If you are Toyota, sole sourcing your supplier is just not a good idea. The Japanese earthquake and tsunami in March 2011 affected the supply chain so drastically that Toyota had to throttle back production, costing the company it's position as the world's number one auto maker. Because of the massive fallout for Toyota, the company is now investing in plans that will reduce their time-to-recovery from the six months that it took during that disaster, to as little as two weeks. According to the plans, Toyota will seek to add dual sourcing for many products, and will work with their sole source suppliers to distribute production across several locations or at least increase the inventory buffers. Further, Toyota will work to develop more "common parts" across many different models of their production vehicles. This will increase the volume of those parts to where suppliers may more reasonably justify building additional manufacturing sites.[21]

This "distribution of manufacturers" works if you are a huge consumer of the goods. You can have a significant impact on your suppliers, and on your manufacturers. But how about if you are an Ice Cream Shop? Say you sole source your ice cream from iSpot A Cow Ice Cream[22], and you are responsible for delivery of the ice cream from a local distributor. What are your supply chain risks?

For the supplier risk, what do you do if the iSpot A Cow manufacturer goes out of business? Well, that might be catastrophic. You will either have to find another ice cream supplier, or buy machinery and hire people to make ice cream. You will also likely have to buy new marketing merchandise, since iSpot A Cow may be listed as your only brand. How can you manage these risks? You can (1) avoid the risk by simply not identifying your business with iSpot A Cow. That way, if anyone comes to your shop, they are not expecting a certain brand. You can (2) reduce your exposure to this risk by having

21 "Global Supply Chain News: Toyota Taking Massive Effort to Reduce Its Supply Chain Risk in Japan", Dr. David Simchi-Levi, March 7, 2012, Supply Chain Digest, http://www.scdigest.com/ontarget/12-03-07-2.php?cid=5576&ctype=content

22 *iSpot A Cow Ice Cream* is a fictitious name, any parallel to a real life company is purely accidental.

several suppliers and advertising in your brochures with all of those company brands. You might be able to (3) transfer the risk. Transferring the risk to an insurance company is always possible, but will certainly cost money. It would be covered in some form of Business Interruption Insurance. You can (4) retain the risk. If iSpot A Cow goes out of business, you will have to decide at that point to close the business, to find a new supplier, and to change your marketing campaigns.

How about if you are an iSpot A Cow franchise instead of an independent ice cream shop that sells iSpot a Cow ice cream? Are you forced to go out of business, or to change your name? This does happen in real life, even for large franchise operations like Bennigan's, and Steak and Ale. It can certainly happen with iSpot A Cow.

4.3 Natural & other external risks

Your company may have potential exposure to weather and natural disasters, traffic disruptions, local disasters. Let's outline a few disruptions that you need to look at.

- Natural disasters include hurricanes, tornadoes, high winds, hail, tsunami, heavy rain, flash floods, mud & rock slides, avalanche, extreme heat, wildfire, earthquake, sink holes, lightning strikes, and drought.
- Traffic disruptions may cause labor issues, delivery issues, and issues with contacting customers.
- Man made disasters include toxic spills (either at your facility, or at nearby facilities), riots, nuclear plant disaster, terrorism, and arson.

Natural disasters can be truly chaotic and tragic events, especially since at times they happen without warning. It is likely impossible to be fully prepared for a natural disaster, since real people are affected in real ways, and those real people may not behave exactly as you have planned. Also, it may or may not matter which disaster hits, it may only matter how the disaster affects your business flow.

For example, what do you do if you come into your retail workplace and a giant sink hole has swallowed the parking lot?[23] Do you have parking privileges with a neighboring business? Or do you have to move your operation to another location? Worse, what happens if customers and employees are in the parking lot when this happens? The immediate emergency takes precedence over any plans you have made.

In a more benign way, what happens if a bridge to one of your customers is out? Do you have an alternate way of accessing the customer site (for example, can you telecommute into your customer's computer system or perform video conferencing), or do you postpone the job until the bridge is back in use? If you are putting a roof on the customer's home, you may simply have to wait it out because the alternative of air dropping the material and employees to that customer's premise is likely unrealistic and too costly.

Let's say you are a licensed Home Health Agency. What is your plan if disaster strikes?[24] In the case of health care, you may have further liabilities and contractual obligations that force you to stay in business. Say a tornado hits your key nursing employee's homes. You may have to augment key

23 "Prattville Sinkhole Affects Area Businesses", WSFA TV, http://www.wsfa.com/story/3156895/prattville-sinkhole-affects-area-businesses

24 "EMERGENCY PREPAREDNESS PACKET FOR HOME HEALTH AGENCIES", The National Association for Home Care & Hospice, 2008, http://www.nahc.org/regulatory/ep_binder.pdf

personnel while they are out on FMLA.[25] Under your contracts with the Agency for Health Care Administration and Medicare, you may be required to remain in business and servicing your patients during a non evacuated hurricane. Or you may simply be required to enroll in the Hurricane Preparedness and Emergency Status System.[26] Regardless, it is important to your business that you know your responsibilities, and your liabilities, during adverse situations.

4.4 Project based risks

There are certain risks that really only manifest themselves when it comes to completing projects. These risks have to be managed, too.

Say you have a small restaurant. Someone has hired you to cater their wedding. You make a big cake for the big event. What do you do if one of your employees drops the cake on the way to the event? What is your backup? Do you transfer the liability in the contract, identifying that if you are not able to meet the deadline you will be liable for a certain amount of money, maybe triple damage based on the purchase price, and make sure you keep your customer informed each step of the way? Do you bake two cakes for the event, deliver each cake in a different vehicle (reducing the effect if one of your deliveries is involved in a car accident)? Do you deliver the cake the day before, giving time to bake a new cake if something goes wrong? Or do you just wing it, tell the people you are sorry, and likely lose your reputation? In any of these situations, communication with the customer is critical. If you've spelled out how you are going to manage the risks and things still go wrong, the customer may be more understanding than if you've worked in a vacuum.

25 "Employee Leave Eligibility and Natural Disasters", Society for Human Resource management, 11/1/2012, By Jeff Nowak, © Franczek Radelet P.C., http://www.shrm.org/hrdisciplines/benefits/articles/pages/employee-leave-natural-disasters.aspx

26 "RE: Hurricane Preparedness and Emergency Status System (ESS) Enrollment – Information Update Needed", AHCA, May 16, 2011, http://ahca.myflorida.com/MCHQ/Emergency_Activities/Files/Hurricane_Preparedness_2011.pdf

5 Conclusions

Small businesses are typically very sensitive to cost. When it comes to protecting your business from disaster, it is great to have backups of backups, and alternates of alternates, but each mitigation requires money, and that money is taken right off the bottom line, the line that should be representing your income.

In this paper, we've presented real life scenarios that impact small businesses. We've looked at four ways to manage risk (avoid, control or mitigate, transfer, or accept). Sometimes changing the way of doing business can have a significant impact on protecting the business from disaster at a small cost. Buying the right equipment or finding the right service provider can have an enduring effect on your success and reducing issues in the first place.

Business Continuity planning has just begun, though. As you gain more experiences with your customers, and as you gain a better insight into your customer's world, you will be able to build even more resiliency into your continuity plans, and reduce the risks that face your business every day. Hopefully reading this paper has given you thoughts on how you can respond in case of crisis, and influenced your thinking when it comes to how your business will survive in times of adversity.

6 References

1. “Emergency Management Guide for Business and Industry”, http://www.fema.gov/library/viewRecord.do?id=1689
2. “How to Create a Business Continuity Plan”, http://www.wikihow.com/Create-a-Business-Continuity-Plan
3. “The six ways of dealing with risk”, http://www.husdal.com/2009/06/13/the-six-ways-of-dealing-with-risk/
4. “Business Continuity Risk Assessment: Risk Analysis Template”, http://www.supremusgroup.com/compliance_template/Risk_assessment_package.htm
5. “Business Continuity Management For Small to Medium-Sized Businesses”, http://www.normit.org/documents/Business%20Continuity%20Plan%20v5.pdf
6. “Why is residual risk so important?”, http://blog.iso27001standard.com/2012/02/13/why-is-residual-risk-so-important/
7. “Business Continuity List of Threats”, http://www.bcmpedia.org/wiki/List_of_Threats
8. "BUSINESS IMPACT ANALYSIS”, http://www.ready.gov/business-impact-analysis
9. "RISK ASSESSMENT”, http://www.ready.gov/risk-assessment
10. "Sample business continuity plan template for SMBs”, http://searchsmbstorage.techtarget.com/Sample-business-continuity-plan-template-for-SMBs-Free-download-and-guide
11. “Division of Services for People with Disabilities Provider Business Continuity and Disaster Preparedness Plan Template”, http://www.dspd.utah.gov/docs/contracttools/DSPD%20Provider%20Business%20Continuity%20and%20Disaster%20Preparedness%20Plan%20Templete%2008-06-07.pdf
12. "BUSINESS CONTINUITY PLAN, University of Connecticut”, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&sqi=2&ved=0CHwQFjAG&url=http%3A%2F%2Fuits.wordpress.uconn.edu%2Fwp-content%2Fuploads%2F2012%2F04%2Fbscnplan.doc&ei=Zxo5UeOJA-WHywHQroHgCA&usg=AFQjCNEzdsoQO7kM8ltfsDbCa02V1ya7Rw&sig2=tiYvrmF8UZHJIw303Rqp9w
13. "SAMPLE Table of Contents and Introduction for aBusiness Continuity Plan”, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&sqi=2&ved=0CGoQFjAE&url=http%3A%2F%2Fwww.nonprofitrisk.org%2Ftools%2Fhallmarks%2Ftools%2F6business-continuity-plan.doc&ei=Zxo5UeOJA-WHywHQroHgCA&usg=AFQjCNG6I4Jlav_wm399hTKgZ1xHEDXdow&sig2=2iHTHBu2EdPNJ4P42Dd2UA
14. "Risk Management vs Risk Avoidance”, https://docs.google.com/viewer?a=v&q=cache:o7xgBI-bPfMJ:www.cs.uwlax.edu/~riley/CS419/RiskMgmt.ppt+&hl=en&gl=us&pid=bl&srcid=ADGEESgVRL2p2i9wVY6XLaQ2SH8yjfU_vOsugfhWB57_UC5eUg7fO0vrW6HxziKZrt904tQ5ajns0LSQkkiuDNemGqKJ-u-4BoOieO-Fbns3WqbEYhyBuAVPNUlJ1Kjuv86xlrGdDHwh&sig=AHIEtbRFzUDFtrSlfvApY3DsZT84sw8ndw
15. "Strategies for successful software development risk management”, https://docs.google.com/viewer?a=v&q=cache:HeDQ2Ow8nUYJ:www.efst.hr/management/Vol8No2-2003/4-boban-pozgaj-sertic.doc+&hl=en&gl=us&pid=bl&srcid=ADGEESiLsNJnkNcIXoo2SoejmLvSwUxlixph9kEU9ZczJPSayGsCAYqQKBtgzZy1g2_F1rik63cDP8DEh2KN3YEy_svv_vk7wu2526uUxouGWMopTy4noOt3fGHykx4EBECvf5ljb3Kf&sig=AHIEtbQgFceqawDmSQVznPG-UPC7Ks7MTA

Appendix A. Business Continuity List of threats

This text is taken directly from "BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR)", List of Threats. "This is a list of possible threats to an organization. From this list, the Organization BCM Coordinator together with the BC Team is required to identify and extract the likely and high-impact threats that will affect your organization. Sometimes, this list of threats may be re-organized into three primary categories of internal and external threats: Malicious activities, Natural disasters and Technical disasters."

- Meteorological (Natural)
  - Blizzard
  - Clouds
  - Cyclone
  - Drought
  - Dust storm
  - Flood
  - Flash Flood
  - Fog
  - Heat Wave
  - Hurricane
  - Lightning
  - Rain
  - Snow
  - Thunder
  - Tornado
  - Tropical storm
  - Weather front
  - Water Spout
  - Wind
  - Wind Storm
  - Fire Storm
  - Fire - Wild, Rural or Urban
- Social (Man-made)
  - Individual Behavior
  - Mass Behavior
  - Terrorism
  - Hijacking in individual, VIP or Group
  - Assassination
  - Torture
  - Poisoning
  - Wounding
  - Bomb
    - Bomb Threat
    - (IED) Improvised Explosive Device
    - Car Bomb
    - Suicide Bomb
  - Biological
  - Nuclear
  - Chemical
  - Cyber
- Technological (Man-made)
  - Transportation Related Events
  - Aviation Accidentson air and ground
  - Rail Accidents occuring above or below ground
  - Maritime Accidents on port, near cost and off the coast
  - Vehicle Accidents
    - Car Accident
    - Multiple Car Accident
    - Bus Accident
  - Information Technology Related Events
  - Hardware Malfunction
  - Software Malfunction
  - Hazardous Materials Related Events
    - During Production
    - During Transportation by road, air, rail, pipeline and sea
    - During Storage
  - Supply Related Events
  - Utilities
    - Power Energy
    - Communications
    - Water
    - Gas
    - Oil
    - Gasoline
  - Food
  - Basic Services
    - Security Services
    - Safety Services
    - Health Services
    - Transportation Services
- Medical
  - Epidemiology
    - Pandemic Flu
    - Dengue Fever
- Geological (Natural)
  - Endogenic
    - Plate Tectonics
      - Earthquake
    - Igneous Activity
      - Volcanic Eruption
  - Exogenic
    - Slope
      - Mass Wasting
      - Landslide
      - Flow
      - Avalanche
      - Mudslide
    - Weathering
      - Erosion

i Open for Business signs taken from
http://sammydvintage.com/thrifting/easy-diy-halloween-costumes/attachment/open-for-business/
http://bucks.happeningmag.com/open-business-after-hurricane-sandy/
http://jan.blog.ocregister.com/2012/05/25/program-seeks-to-turn-unemployed-into-self-employed/79385/open-business-560/
http://www.adventuresinoss.com/?p=2256