10 Steps for Surviving a Disaster!

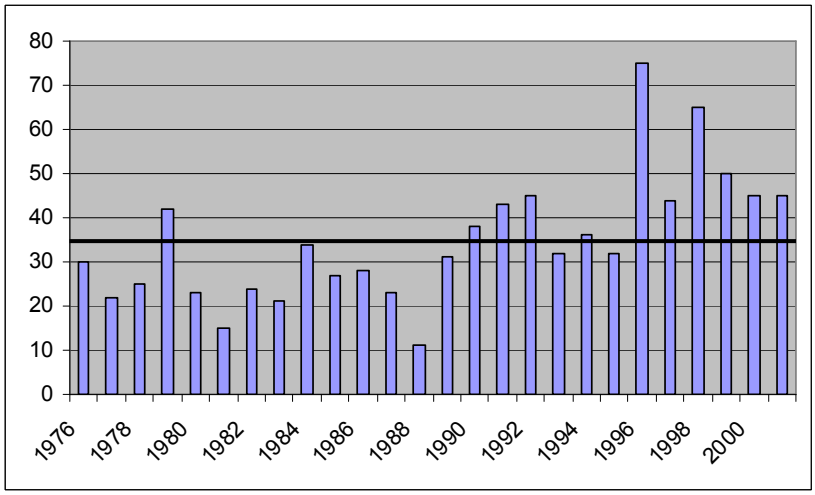
By Vin D'Amico, Principal
DAMICON, LLC

This article was published in the 2004 *Handbook of Business Strategy*.

If a critical part of your business was knocked out of commission for a few days, would your business survive? What would you do during that time? Close the doors? Take orders by hand? Refer people to a competitor? How much business would you lose? How quickly could you recover?

Disasters happen! Floods, fires, storms, accidents, outages, whatever. And it's not just about you. A disaster could hit one of your key suppliers or a major transportation service provider. Suddenly you can't deliver. How you and your firm react will determine your fate. Your customers will still want their orders filled and services provided, and if you can't come through, they'll go somewhere else!

When you hear the word disaster, you probably think about stories on the 6 o'clock news. The Federal Emergency Management Agency (FEMA), which is responsible for responding to federally-declared disasters, has counted an average of about 35 disasters per year going back to 1976 (see the accompanying bar chart).



FEMA DISASTER ASSISTANCE EFFORTS

The likelihood of your company being impacted by such a widespread disaster is quite small. You need to be more concerned about everyday events that have the potential to seriously disrupt your business. What can go wrong? Take a look at the following table.

Deleted: (FYI: they like graphs but will be printing in black and white. You can submit this or a bw version but just wanted you to eb aware: no color.)¶

What can go wrong?	
Equipment/Software Failures ▪ Software failure ▪ Network outage ▪ Hardware failure ▪ Any critical device breakdown **Natural Disasters and Accidents** ▪ Fire ▪ Flood ▪ Storm ▪ Tornado ▪ Earthquake ▪ Chemical contamination **Human Error** ▪ Lost files ▪ Access denial ▪ Data corruption ▪ Overwritten data	**Malicious Acts** ▪ Bombing ▪ Computer virus ▪ Stolen equipment ▪ Employee sabotage ▪ Denial of service attack **Utility Problems** ▪ Burst water pipes ▪ Power outage/surge ▪ Heating system failure ▪ Air conditioning failure ▪ Communications outage **Business Crises** ▪ Product defect ▪ Supplier disruptions ▪ Transportation problems ▪ Major customer/supplier bankruptcy

You get the idea. More things can go wrong than you care to think about. This table is not intended to be an exhaustive list but it gives you plenty to think about. When you include your key suppliers, transportation firms and even major accounts in the scenario evaluation, the risk that your business will be severely impacted by a disaster is too large to be ignored.

Here are a few statistics regarding computer system disasters that should awaken you to the level of risk you face.

- A computer hard drive crashes every 15 seconds.
- One in five computers suffer a fatal hard drive crash during their lifetime.
- Around 2,000 laptops are stolen or lost every day.
- As much as 60 percent of corporate data resides unprotected on PC desktops and laptops.
- 60 percent of companies that lose all their data close down within six months of the disaster.
- PCs are infected by viruses at a rate of more than 10 percent each month.
- 37 percent of users reported loss of data due to viruses.

IT CAN HAPPEN TO YOU!

Deleted: (

Deleted: -?)

Disasters are unavoidable. Sometimes it's as simple as a leaky roof, severe weather or a traffic accident. Most computer system outages are triggered by minor incidents like broken water pipes, fire and smoke damage, electrical equipment failures, or computer viruses.

Sometimes a large geographic area is impacted such as the Great Northeast Blackout of '65, the Northeast Blizzard of '78 or the nationwide AT&T network failure of '90. It's inevitable. Your business will be impacted by a disaster of some kind before long.

Facts: According to the Association of Records Managers and Administrators, about 60 percent of businesses that experience a major disaster such as a fire close within two years. According to Labor Department Statistics, over 40 percent of all companies that experience a disaster never reopen and more than 25 percent of those that do reopen close within two years.

When your customers are forced to buy from someone else because you can't deliver, they will view your competitor as a savior, someone who bailed them out. That attitude creates a sense of loyalty that you will have an extremely difficult time overcoming. Don't let this happen to you!

Obviously, prudence dictates that you take appropriate steps to prevent disasters that you have some control over. When, for example, was the last time the roof was inspected? You should also check insurance coverage types and levels.

But that's not going to be enough. No amount of disaster prevention planning will guarantee safety. So let's turn our attention to surviving a major disaster.

TEN STEPS COULD SAVE YOUR BUSINESS

The steps that follow are based on three critical elements for creating an effective survival strategy: people, process and technology.

(1) Preparing to deal with the human factors is the single most important aspect of surviving a disaster. People are your organization's most valuable asset. Reassuring and educating them in advance of an emergency situation is the first critical success factor. By defining how people should react to a crisis and providing them information and tools to manage that reaction, the impact will be lessened and the transition to emergency operations smoothed.

Ten Steps for Survival

People
1. Assemble a multi-disciplined planning team
2. Name a sponsor and a planning team leader
3. Define roles and recovery team participants

Process
4. Catalog your business processes
5. Conduct an impact analysis
6. Assess business survival options
7. Document and test the survival plan

Technology
8. Identify critical systems
9. Examine system administration procedures
10. Consider redundancy options

(2) The next major element is process. There are dozens, hundreds, perhaps thousands of business processes that your organization executes every day. Some are mission-critical, some are secondary and the rest are supportive. You'll need to define which processes really matter to your business and how you'll keep those processes operating when disaster strikes.

(3) Finally, there's the technology element. I'm not just referring here to computers and software. You also need to consider production machinery, network equipment, printers, telephones, fax machines, copiers, etc. Some or all of this technology may be unavailable during a disaster. Don't let your business succumb to a technology failure. There are a variety of options available to you.

The sidebar "Ten Steps for Survival" gives you a quick summary of the steps you need to take in order to thrive during a disaster. Let's go over them in detail.

PEOPLE

When disastrous events occur, most people stop. They don't know what to do or how to react. It's the "deer caught in the headlights" effect. Your planning efforts will minimize this behavior. Ultimately, your people are the most important factor in surviving a disaster. They need to be confident that the company can get its job done no matter what. So, focus on the people factors first.

1. Assemble a multi-disciplined planning team

The planning team will create the roadmap for managing a disaster. Which departments to include on the team will vary from company to company. Consider representation from customer service, facilities, finance, human resources, manufacturing, network management, operations, purchasing, sales, security, and/or systems administration. The idea is to identify a mix of skills within the company. The team will define business requirements, analyze the business impact of various disaster types, design the survival process, identify members of the recovery team, document the survival plan, and oversee testing of the plan.

Make sure you have a good cross-section of roles and levels within the organization. You need people on the planning team who are intimately familiar with company operations. Your management staff alone may not know enough of the details to create a thorough survival roadmap.

2. Select an executive-level sponsor and a planning team leader

This is important! Someone on the executive management team must be an active participant in the planning process. The efforts required will span the entire company and require cooperation from multiple departments. This person must be able to clear roadblocks and resolve issues.

The planning team leader is the point person for the disaster survival process. The team leader must assemble the multi-disciplined planning team and lead them in developing business survival strategies. This person should be a good leader with enough knowledge of the business to be able to ask the right questions and seek out cost-effective answers.

3. Define roles and choose participants for the recovery team

The recovery team is responsible for overseeing execution of the survival plan. Team members coordinate survival activities and lead the recovery efforts within their respective operational areas. They will choose the individuals to perform specific survival activities after any declared disaster. The recovery team leader must have the authority to make quick decisions and draw upon whatever resources are needed. The recovery team may be similar to the planning team. However, you should think about including representatives from key customers, suppliers and outside service providers on the recovery team.

Why include people outside the company? Your customers, suppliers and other providers will need to be informed if a disaster occurs that impacts their businesses. As part of the recovery team, large customers can help manage order flow and work around short-term supply disruptions. Likewise, suppliers may need to hold or re-route shipments. Maybe, they can even ship directly to your big accounts! Take full advantage of your suppliers.

Various other service providers will be able to help you keep operating by providing alternate means of conducting business (see step 8). Once the recovery team is selected, roles and responsibilities must be clearly communicated to all inside and outside the company.

PROCESS

Let's turn our attention to business processes. You'll identify the mission-critical processes. These are the ones that represent the backbone of your business. Each process will need people, technology, and logistics to operate effectively. People needs include specific roles and responsibilities that execute a process. Technology needs include essential hardware and software systems for automating the process. Logistics needs include transportation to and from the disaster site as well as a separate recovery site, if one is included in the plan.

4. Catalog your business processes

A disaster survival plan can't justify the expense of including every business process, each piece of equipment and all software applications in the survival effort. Take an inventory of major business processes for the entire company. Ask middle and senior level managers to define the activities within their departments that are most critical to the business. For example, the sales and marketing groups will want to keep all selling channels available. The finance group will want to keep payables and receivables moving.

Disagreements will erupt. Do you really need ALL selling channels? Are collecting on invoices and processing payables critical activities during a brief business disruption? Think about what really matters to your business. Remember, we're talking about survival here. Processes that don't make the inventory list may be vital to the long-term success of the company but not critical to short-term survival.

At first, don't try to prioritize or make a deep value judgment on these processes. Just get them defined. When in doubt, add them to the list. The impact analysis that follows will tell you what's mission critical.

5. Conduct an impact analysis

Now that you know what the major processes are, you need to ask a question about each one. What would be the impact on the business if this process could not be performed for several days? Now prioritize your business processes based on the impact analysis. Use three levels of priority. For example:

A) Processes that need to be resumed within 24 hours to prevent serious business impact, such as loss of revenue or a serious adverse impact to customers.
B) Processes that need to be resumed within 72 hours to maintain near normal operations and adequate levels of quality.
C) Processes that can take more than 72 hours and may not be needed at all unless the disaster is unusually long.

The 24 and 72-hour timeframes may not be appropriate for your situation. Shorter or longer durations may apply.

Story: Most disaster scenarios are short-lived. The following outages had a common cause, the Slammer virus attack of January 2003. Bank of America: ATMs knocked out for a day. Continental Airlines: Flights delayed or canceled due to ticketing and check-in problems. City of Seattle: 911 network knocked out for a day. Washington Mutual: ATMs knocked out for two days. Seibel Systems: Moderate to severe network problems for three days. These types of brief disruptions can cause lost customers, frustrated employees and damaged equipment. 24-72 hour disruptions are what you should be most concerned about.

6. Assess business survival options

Based on the impact analysis, consider multiple business survival strategies. Think about manual processing options, engaging an outside firm to take over some or all operations, establishing a remote, redundant site for mission-critical operations, or even sending customers to a competitor with whom prior arrangements have been made (such as: "I won't steal your customers and you won't steal mine."). To protect yourself against a key supplier or transportation firm being hit by a disaster, consider using a secondary organization for some percentage of your workflow. Even if you gave a backup supplier just 5 percent of your orders, they would be familiar with your needs and able to move quickly in the event of trouble with the primary source.

As part of this step, define the specific criteria for declaring a disaster and who is authorized to make the declaration. Create a procedure for determining which business processes are impacted by the disaster. Be ready to act quickly and decisively. If a major disruption occurs, time is your enemy! Consider a phased approach whereby you might declare a "pending disaster" at the earliest stages when you're not quite sure about the impact an event will have. This gets your team mobilized, minimizes losses and accelerates return to normal operations.

This step also requires creating an emergency call list. The person declaring the disaster must notify key personnel who in turn may be asked to notify others. This distributed notification approach enables rapid dissemination of information resulting in rapid emergency response.

7. Document and test the survival plan

Don't write a book. Keep the documentation simple and actionable. This document will have to evolve over time so you don't want to create a large maintenance task. Include network configuration diagrams, company directory, roles and responsibilities for the recovery team (see step 3), and specific survival procedures. The recovery team will have responsibility for maintaining the accuracy, accessibility, and distribution of the survival plan.

At least once a year, try out the plan. Conduct a mock disaster. Walk through the plan and be sure it's still valid. Your business will evolve and grow. The plan will have to change too. You may find that you need to make arrangements for offsite or third-party support to fully implement the plan. That may take several months requiring that you think about some short-term survival procedures while the long-term plan is created.

Always conduct a postmortem after each test. This effort will surface needed improvements in the plan to keep your business running in the event of a disaster.

Story: In 1996, Omega Engineering suffered a catastrophic manufacturing systems failure due to a malicious act by a recently-fired employee. The company had a well-defined backup procedure and stored the tapes in a cabinet onsite. Unfortunately, the backup tapes were missing in this case. The failure cost Omega in excess of $10 million.

While malicious employee behavior cannot be entirely prevented, proper procedures can minimize the after-effects. Consider involving multiple employees in any mission-critical process so that lone malicious acts are difficult to accomplish.

TECHNOLOGY

Finally, you need to have an understanding of all the physical assets that support each process. In a disaster, some or all of those assets may be unavailable.

8. Identify critical systems

Your business is likely to have many desktop and server computers. There are also firewalls, routers, switches, printers, scanners, fax machines, copiers, telephones, and so forth. Determine which of these devices are truly critical to your business. Criticality is measured by your ability to conduct business without that device.

Is there a substitute device, for example, using a mobile phone instead of a landline? Can the work be done just as well manually though at reduced speed? Would one of your business processes be completely unavailable without some piece of equipment? You may need to identify alternate equipment and suppliers who can respond quickly in a crisis.

Story: The New York court system quickly switched over to wireless connectivity and voice-over-IP (VOIP) technology after September 11, 2001 to maintain critical communications systems. Canon U.S.A. set up a laser-based communications link that ran between satellite dishes to replace a data connection that was severed between two court buildings. Meanwhile, Nortel Networks shipped 600 VOIP telephones to replace the more than 2,200 downed telephone lines at the courthouses in Lower Manhattan.

Do you have an intranet web site as well as an Internet web site? In a disaster, forget the intranet. Confiscate the server for use on the Internet web site. Fax machines or copiers out of commission? Do you have a desktop scanner? Convert a PC into a combination fax and copy machine. Be creative!

In a manufacturing operation, having multiple manufacturing sites spread over a wide geographic area is the best bet. Alternatively, you could use a contract manufacturer for a portion of your production. They would then be a back-up production source in the event your primary plant is out of commission.

9. Examine system administration procedures

Review how your major systems are maintained. It is quite surprising how simple disasters can often be avoided by following proper administration procedures. Are your computers backed-up regularly? Are the backup media stored offsite? Do you have antivirus software installed and updated regularly?

Don't forget about the paper files. Are copies stored offsite? Have you digitized and archived them for safety? Can your business operate without them?

Story: When a massive flood hit the Morgan Library at Colorado State University in 1997, computer systems were soaked and data was lost. The good news is that regular back-ups had been done. The bad news is that those back-ups were not stored offsite. Unfortunately, the back-ups were also heavily damaged and unusable.

All of the above is about physical or tangible assets. What about the intangibles - knowledge, know-how, creativity, relationships, etc.? Do you have employees who know critical information about the business that's not documented anywhere? If so, you are far more exposed than you may think. In a disaster scenario, people will need to cover for each other. They can only do that if information is written down. Turn those intangible assets into tangible form before it's too late.

10. Consider redundancy options

Finally, think about duplicating or mirroring critical systems. This can be done onsite and/or offsite depending on the needs of the business. The subject of "failover" (switching to a redundant system when the primary system fails) is complex and the solutions can be very expensive. If your customers depend upon you for 24x7 operation or you have contractual obligations for such, then redundancy is essential.

Story: 300 companies were affected by the February 26, 1993 bombing of the World Trade Center in New York. According to a Gartner report, 87 percent did not have a disaster recovery plan. A shocking 58 percent of those without a plan were out of business within one year. The New York Board of Trade (NYBOT), a commodity trading exchange, was located in the World Trade Center. They had a plan, put it into action and made it through. It took a couple of days to begin trading again but at least they could conduct some business.

Lessons learned convinced them to upgrade the plan. They established a goal of switching to a redundant site within hours, not days. Then disaster struck again. Within 24 hours of the devastation on September 11, 2001, the NYBOT was back in business. They had a survival plan, tested it quarterly and invested in a redundant site in Queens, NY at a cost of $300,000 per year. Sound expensive? Not when you consider that it costs them $350,000 per day to be out of commission and it costs their partners 10 times that amount!

EXPLORE, PLAN, EXECUTE, VERIFY.

Once you've completed the Ten Steps for Surviving a Disaster, you'll be ready to face any severe disruption to your business with confidence. You've explored the options, planned for the worst, executed a test and verified the results. You're ready!

One final note - any time you undertake a major new business initiative, make survival planning part of the project. For example, if you're about to invest in a new software application to expedite customer orders and tracking capabilities, evaluate multiple failure scenarios. What new vulnerabilities does the software expose? How will orders get processed and tracked if the new system is unavailable? Technology is a valuable asset to your business. Make sure you're in control of it at all times. Don't let a disaster take your business down with it!

It's never easy to face the curve balls that Mother Nature, malicious people and pure chance throw at you. But if you're prepared, you'll be a survivor!

Vin D'Amico is Founder and President of DAMICON, LLC, your ADJUNCT CIO™. He is an expert in leveraging open software to drive growth. DAMICON provides Freelance Technical Writing, Disaster Response Planning, and Security Management services to firms throughout New England. Vin can be reached at vin@damicon.com or by visiting www.damicon.com.

You can learn more about the Handbook of Business Strategy at http://www.emeraldinsight.com/hbs.htm.