Faster Disaster Recovery

The Business Owner's Guide to Developing a Business Continuity Plan

JENNIFER H. ELDER, SAMUEL F. ELDER

AICPA

WILEY

Faster Disaster Recovery

Faster Disaster Recovery

The Business Owner's Guide to Developing a Business Continuity Plan

Jennifer H. Elder
Samuel F. Elder

AICPA®

WILEY

Cover image: © Andrew Burton/Staff/Getty Images
Cover design: Wiley

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993, or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

ISBN 978-1-119-57096-7 (Paperback)
ISBN 978-1-119-57102-5 (ePDF)
ISBN 978-1-119-57094-3 (ePub)

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

This book is dedicated to our families. Thank you, Brian and Eunice Howard, Judith Mernick, Gaynor Sorrell, Dr. Samuel and Sandra Elder, Susan Alders, and Chris Elder. Without your wisdom, advice, and support, we would never have survived the disasters!

Contents

Preface

Every year, disasters, emergencies, and disruptive events take a toll on organizations around the world. They cost money and lives and, too often, organizations never recover.

Although we may not be able to do anything to stop a natural disaster or keep the most sophisticated hackers from attempting to steal our confidential information and trade secrets, there are *many* steps an organization can take to reduce (and even prevent) damage, enabling them to perform business as usual.

Certainly, a disaster can be created by a massive event, such as a hurricane, fire, or terrorist attack, but it can also be triggered by smaller events, such as a power outage, cyberattack, or even road construction.

And in many cases, disastrous events can be predicted and the extent of their impact expected. For instance, hurricanes like Superstorm Sandy (which hit the East Coast in October 2012), Hurricane Maria (which hit the Caribbean and Puerto Rico in 2017), or Hurricane Harvey (which hit Texas in 2017 and caused $125 billion in damage, mostly in Houston), are often tracked and monitored as they develop.

Although Superstorm Sandy was predicted, no one expected that power would be out for 9 to 12 weeks in many areas of New York and New Jersey. And Hurricane Maria was predicted, but the effect was not something many businesses were prepared to handle. How do you open your store if your employees cannot get to work? How do you find employees when many of the island residents decide to relocate to another country? How do you open your manufacturing facility if you are without power for six months? Would your business survive?

However, although some disasters can be foreseen by experts, they are often overlooked by businesses and organizations. If your organization is located near a bridge, for example, have you ever considered the impact of a closure?

According to a 2018 report by the American Road and Transportation Builder's Association,[1] 54,259 of the bridges in the United States are rated "structurally deficient." And one in three bridges have identified repair needs. It only makes sense that if a bridge is known to be structurally deficient before a disaster, the disaster is likely to make it worse, maybe even totally destroying it. This can greatly impact your company, as one business owner in Maryland learned the hard way.

This particular woman was a veterinarian who lived on one side of a small, two-lane bridge; her practice was on the other. One day, the bridge failed unexpectedly, closing it for nine months for repairs and turning her normal five-minute drive to work to a full 45-minute nightmare.

While she personally found this annoying, she discovered that her customers found it *impossible*, largely because they didn't want to subject their sick pets to a longer car ride, especially in the event of an emergency. As a result, her revenue dropped by a greater percentage each month the bridge was closed. Ultimately, she wound up losing 30 percent of her annual revenue . . . and many of her loyal customers.

Admittedly, this same disaster may not have the same impact on every organization, as what may be an annoyance for one can be a crisis for another. For instance, your computer servers going down is likely to be bothersome, but if you have a bank or brokerage, you may never recover from such a disaster.

Additionally, a winter storm bringing three feet of snow may have no impact on an organization if the employees can work virtually from home, but how do hospitals function if their employees can't get to work? What happens then?

Aside from additional expenses and lost revenue, another often-overlooked impact of a disaster is reputational loss. Your hard-earned, stellar reputation for reliability and dependability can be permanently damaged if you're unable to react quickly to a disaster and address the needs of customers and employees.

That's why this book exists—to help business owners like you protect your company's reputation as well as your finances in the event of a disaster. Each chapter discusses a different area of disaster planning of a business continuity process. At the end of each chapter is "Questions to Ask Yourself" to help you apply what you learn to your organization.

NOTE

1. The ARTBA 2018 Deficient Bridge Report, https://www.artbabridgereport.org.

CHAPTER 1

Business Disaster Defined

How do you define a disaster? What about a *business* disaster? Is it different? Or is it the same?

As pointed out in the preface, although this is a relevant question—especially in this day and age where disasters seem to make the news weekly, if not daily—it's one that a number of businesses choose to ignore.

Technically, a business disaster can be defined as:

1. Any unplanned interruption of normal business functions or processes for an unacceptable period of time.
2. A situation or event that overwhelms capacity and/or necessitates a request for external assistance.

In either case, when an organization or a department within an organization can't function normally, it's incurring extra expenses, losing revenue, or both. None of these are good.

When breaking down the definition, it's important to understand that every company defines "interruption" and "unacceptable period of time" differently.

For example, an accounting firm may be able to function without access to data files for 24 hours, whereas a financial institution may find being without data for more than 20 minutes totally unacceptable.

According to the Federal Emergency Management Agency (FEMA), a disaster is "any unplanned event that can cause deaths or significant injuries to employees, customers, or the public; or that can shut down your organization, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public image."[1]

Based on this definition, a disaster involves any event that disrupts your company's normal operations, or that limits or prevents access to company information and systems.

DISASTER TIMING AND SIZE

Disasters are inevitable in most businesses, but the problem lies in the fact that their timing is frequently unpredictable. This means that, although they *can* happen with some notice or warning, they typically happen when we least expect it.

With a hurricane, for instance, you may have several days or a week to prepare. With a tornado, you have seconds. Some disruptions—such as power outages or computer viruses—can occur with no warning at all.

Disasters also come in all shapes and sizes. Although we often think of them as large in scale, affecting thousands or millions of people, even small events can quickly become a disaster for a company.

A computer virus, water main break, the loss of a supplier, or the arrest of a company officer for driving while intoxicated can dramatically affect the finances of an organization.

The size and nature of the company can also affect the impact of a disaster. For instance, a newspaper article describing the discovery of a $100,000 case of fraud might not have a huge effect on a multinational company, but it will likely *severely* impair the finances of a nonprofit.

DISASTER TYPES

The types of threats that occur when a disaster strikes can be broken down into seven different categories:

1. **Environmental—**hurricane, tornado, or flood
2. **Biological—**illness, such as flu
3. **Deliberate—**workplace violence, bomb threat, or fraud
4. **Utilities—**loss of power or telecom services
5. **Equipment—**breakdown or inability to obtain spare parts
6. **Information Technology—**hardware failure, data loss, or cybercrime
7. **Other—**labor disputes, road closures, or the loss of key personnel

Each of these can have a major impact on how a business runs. Each one can also cripple a company, which is why it is absolutely critical to create a disaster plan, preferably before you need it.

Questions to Ask Yourself

1. How do you define a “business interruption”?
2. What would you consider an “unacceptable period of time”?
3. What disasters do you face that are often predicted, giving you some lead time?
4. Which disasters tend to creep up, essentially appearing out of nowhere?
5. What types of disasters could potentially cripple your company?

NOTE

[1] “Emergency Management Guide for Business and Industry,” Federal Emergency Management Agency (October 1993), https://www.fema.gov/media-library/assets/documents/3412.

CHAPTER 2

Why You Need a Plan

Physical damage from natural disasters is often the first thought that comes to mind. Yet, there are many financial effects that can have a substantial negative impact on an organization.

Employees may not be able to come into work. Customers may not be able to get to your location. Data and records may be permanently lost. Utilities may be down for weeks. Suppliers may be displaced.

A good disaster response plan, also called a business continuity plan (BCP), addresses these potential issues from a broad perspective. But why go through the time and energy to create this type of plan?

DISASTERS OCCUR . . . A LOT

According to the World Health Organization, across the globe 160 million people are affected by disasters and 90,000 people are killed annually.[1]

According to the Federal Emergency Management Agency (FEMA), in 2017 disasters affected 8 percent of the population of the United States. If you were not affected personally, your family or friends likely were; 2017 saw FEMA responding to 59 major disasters and 16 emergency declarations.[2]

According to the Center for Research on Epidemiology of Disasters (CRED), 2017 saw 318 natural disasters in 122 countries affecting 96 million people and costing $314 billion.[3] Figure 2.1 provides a visual representation of the 2017 disasters. The statistics go on and on, but I think you get the idea—disasters are here to stay. Most people have experienced a disaster either personally or professionally (and sometimes both!). Consider yourself lucky if haven't, but also consider yourself forewarned.

Although the number of geophysical disasters (earthquakes, volcanoes, rock falls, landslides, and avalanches) has remained relatively stable, hydro-meteorological disasters like floods, storm surge, heat and cold waves, drought, and wildfires have increased dramatically.

This means that in order for your organization to cope with the initial event and survive in the long term, you need to be prepared. Or, as the old saying goes, "failing to plan is planning to fail."

As seen Figure 2.2, during the 10-year period from 2007 to 2016, there were 354 natural disasters. In 2017 there were 335.

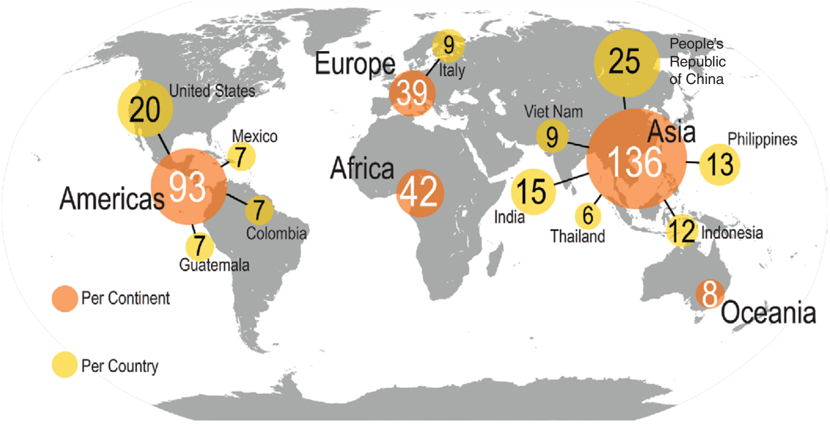


Figure 2.1 Number of Reported Disasters by Country
Source: "Number of Reported Disasters by Country," Center for Research on Epidemiology of Disasters, March 2018.

Figure 2.3 is a chart showing the number of reported natural disasters from 1900 through 2017. As you can see, the number of disasters is increasing at an exponential rate.

Freak storms are on the rise in the United States as well. In 2004, four major hurricanes—Charley, Frances, Ivan, and Jeanne—all struck Florida in just six weeks.

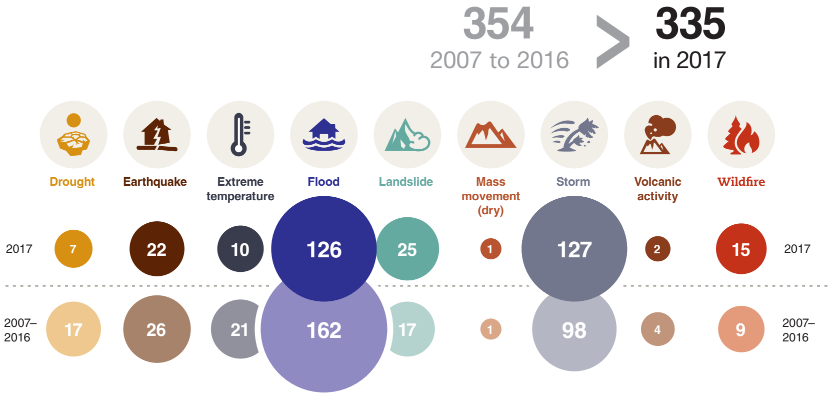


Figure 2.2 Occurrence by Disaster Type: 2017 Compared to 2007–2016
Source: "Natural Disasters in 2017: Lower Mortality, Higher Cost," Center for Research on Epidemiology of Disasters, March 2018.

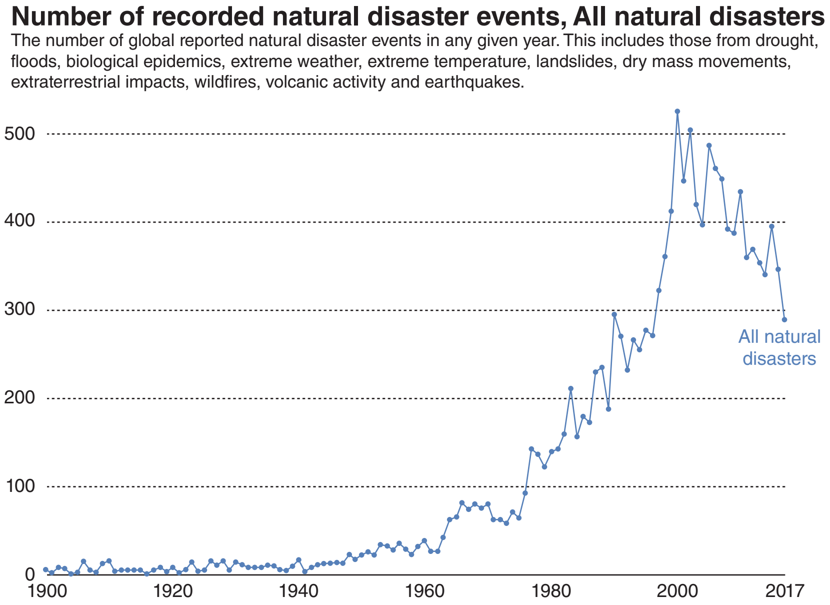


Figure 2.3 Reported Natural Disaster Events by Year
Source: "Natural Catastrophes," Hannah Ritchie and Max Roser, Our World in Data, https://ourworldindata.org/natural-catastrophes.

In July 2011, a dust storm known as a *haboob* hit Arizona, shutting down the Phoenix airport for 45 minutes. The dust wall was estimated at 5,000 feet high by 60 to 70 miles wide.

And in June 2012, a violent and fast-moving string of thunderstorms, known as a *derecho*. With peak winds of 91 miles per hour, the derecho was equivalent to a Category 1 hurricane. When all was said and done, it left a 700-mile swath of downed trees and power lines all the way from the Midwest through the mid-Atlantic states. Extensive damage occurred in Indiana, Kentucky, Ohio, Pennsylvania, West Virginia, Virginia, District of Columbia, Maryland, Delaware, and New Jersey. The 2-day storm resulted in 22 deaths, and almost 5 million customers were without power, some for 5 days or more. How would your business respond if you were without power for almost a week?

In October 2012, Superstorm Sandy had winds extending 1,100 miles, affecting 24 states (the entire eastern seaboard from Florida to Maine and as far west as Michigan and Wisconsin) and knocking out power to approximately 8.5 million homes and businesses. Superstorm Sandy claimed 233 lives and cost $72 billion.

In September 2013, areas surrounding Denver, Colorado, received upward of 15 inches of rain in one week, resulting in flooding in 14 counties over 200 miles that damaged 1,500 homes.

That entire year was a busy one for disasters, with the German insurance company, Munich Re, reporting that there were 880 major natural disasters around the world in 2013. All in all, they killed an estimated 20,000 people and cost $125 billion in damage.[4]

Worldwide, 2013 was also the year of at least 11 major earthquakes of 4.7 magnitude or greater. There were also several other "earth-shaking" events, including a fertilizer plant explosion in Texas that created a 2.1 magnitude tremor felt in 36 different zip codes and a meteor explosion in Chelyabinsk, Russia, which generated a shockwave that damaged an estimated 4,000 buildings and injured more than 1,000 people.

Paul Caruso, a geophysicist with the U.S. Geological Survey[5] reports that, in the first week of April 2014, Oklahoma—a state known more for tornadoes—experienced 48 quakes of 2.5 magnitude or above. During the prior 30 days, there had been 157 quakes larger than magnitude 2.5, whereas, in 2009, only 50 earthquakes were reported for the *entire year.*

After 12 years of little to no hurricane activity, 2017 saw the most active and costliest hurricane season since 2005. Hurricane Nate was the costliest disaster to ever hit Costa Rica. Hurricanes Harvey, Irma, Maria, and Nate had their names retired due to their high damage costs and loss of life.

There's also the issue that some states tend to have more major disasters than others. As Table 2.1 shows, there are 10 states that top the charts for the number of disasters declared since 1953.

DISASTERS HAPPEN QUICKLY

Many types of disasters have little or no warning: sabotage, Internet outages, tornadoes, and earthquakes. When a disaster strikes, you and your employees are dealing with extreme levels of stress, anxiety, fear, and sadness. You may be dealing with information overload or a complete lack of information.

Table 2.1 Ten States Most at Risk for Natural Disasters

State	Types of Disasters	No. Declared Since 1953
1. California	Earthquake, wildfire, landslide, flooding, and severe freeze	281
2. Texas	Tornado, flooding, hurricane, and wildfire	255
3. Oklahoma	Tornado, wildfire, winter storm, flooding, and terrorist bombing	173
4. Washington	Wildfire, winter storm, volcano eruption	136
5. Florida	Hurricane, wildfire, and severe freeze	130
6. New York	Winter storm, flooding, hurricane, and terrorist attack	95
7. Alabama	Hurricane and tornado	82
8. (tie) Colorado	Wildfire, snowstorm	80
8. (tie) New Mexico	Wildfires	80
10. (tie) Louisiana	Hurricane and flooding	79
10. (tie) Oregon	Flooding and wildfires	79

Source: Megan Trimble, "America's 10 Most Disaster-Prone States," *US News and World Report,* June 18, 2018.

The chaos alone is enough to make it harder to think clearly, quickly, and smartly. According to Earl Miller, a neuroscientist at Massachusetts Institute of Technology, switching between just two tasks can reduce your IQ by 10 points![6] Now imagine the effect if you are multitasking all day, all week, and under extreme stress.

In October 2018, a tropical storm was swirling in the Gulf of Mexico. Many forecasters did not expect much from it. The last time a hurricane had hit the Panhandle was in the 1800s. Forecasters thought it might reach Category 1 status at best. Unfortunately, they were very wrong.

In less than two days, the tropical storm became Hurricane Michael—a Category 4 hurricane with maximum sustained winds of 155 mph. It continued into Georgia with 115 mph winds and even into Virginia with 75 mph winds. That little tropical storm became Hurricane Michael, the third most intense continental U.S. landfall by pressure and the fourth strongest by wind speed.[7]

It left the Florida Panhandle in ruins, entire blocks of homes and businesses flattened, roofs peeled off, windows blown out, merchandise blown away or destroyed.

Unfortunately, with so little warning many people and businesses had no idea what to do. Many people did not even evacuate because they had no idea where to go or what to take. Many businesses just closed their doors and hoped for the best, only to find out that their building was no longer standing and all their records were destroyed. The owners may have survived one disaster only to come back to another one entirely.

Businesses with a disaster plan have checklists they can follow quickly that can minimize the damage or at the very least ensure that they have the information they will desperately need once cleanup and recovery begin.

DISASTER RESPONSE IS EXPENSIVE

Not only have these types of disasters impacted these states in greater proportions, they've left lasting financial impacts as well. Case in point: here are the 10 most expensive natural disasters in the United States, as well as their costs:

1. Hurricane Katrina, Louisiana, 2005 (*$165.8 billion*)
2. Hurricane Harvey, Texas, 2017 (*$127.5 billion*)
3. Hurricane Maria, Puerto Rico and St. Croix, 2017 (*$91.8 billion*)
4. Superstorm Sandy, East Coast, 2012 (*$72.2 billion*)
5. Hurricane Irma, Florida, U.S. Virgin Islands, 2017 (*$51 billion*)
6. Hurricane Andrew, Florida, 1992 (*$49.1 billion*)
7. Flooding, Midwest, 1993 (*$33.8 billion*); drought and heat wave, Midwest, 1988 (*$43.4 billion*)
8. Flooding, Midwest, 1993 (*$36.9 billion*)
9. Hurricane Ike, Texas, 2008 (*$35.7 billion*)
   Hurricanes Rita and Wilma, Gulf Coast, 2005 (*Tied; $19 billion*)
10. Drought and heat wave, Midwest, 2012 (*$33.3 billion*); Hurricane Charley, Florida, 2004 (*$18.5 billion*)[8]

After a disaster, organizations may have to deal with many difficult financially impacting problems simultaneously. Loss of sales, loss of customers, loss of vendors, increased materials costs, decreased employee productivity, lack of employees, and damage to reputation can all occur.

Then there's the added burden of dealing with increased financial needs *while* cash flows are reduced. You may need to pay for cleanup and replace damaged equipment and inventory. Material costs might also be much higher due to the sudden increase in demand.

Add that to the regular and ongoing fixed expenses that still continue to accrue. Rent, mortgage payments, real estate taxes, utility bills, and loan payments all still have to be paid. Some companies even continue to pay their employees when they can't come to work.

Sadly, many organizations mistakenly believe that insurance and/or government aid will be sufficient to get back up and running. Yes, once you've exceeded your deductible, your insurance will likely cover *some* of your expenses, but it likely won't cover them all. Plus, many disasters aren't covered without a specific rider.

Sometimes the coverage and support you receive comes too late because it takes time for insurance companies to process claims. If the disaster affects many people, as is often the case with a hurricane or flood, you may wait as long as six months to two years to receive full payment. By then, your doors could be closed.

Failing to address these additional cash needs ahead of time means that you may not have many options for finding necessary funding when you need it most.

Banks may have difficulty granting a loan to a company without revenue, even if the shortfall is temporary. And damaged assets don't normally make the best form of collateral.

Sure, some lenders may be willing to provide a short-term, unsecured loan to assist, but the terms will likely be expensive. Can you cover the costs?

Or what happens if the property financed by the lender was destroyed? In this case, the lender may seek full repayment of the loan prior to receiving any insurance coverage payouts. That's if the insurance proceeds even cover the remaining balance due.

As one might anticipate, bankruptcy filings increase substantially in the five years following a disaster. Robert Lawless, a professor at the

University of Nevada at Las Vegas, reports that in states directly hit by a hurricane, bankruptcies go up by 50 percent. *For states with tangential damage, there is still a 20 percent increase.*

IMPAIRED RESPONSE

Bertrand Russell once said, "The dread of a disaster makes everybody act in a way that increases the disaster." By their very definition, disasters create disarray and uncertainty. Their emotional toll alone not only decreases productivity, but also makes decision making more difficult.

The accompanying lack of sleep and sadness has a negative effect on the quality of decisions made. After all, it's exponentially harder to figure out what to do in the *middle* of a disaster when everything and everyone around you is in chaos and emotions are running high.

In many disaster scenarios, the power, cell towers, and telephone lines go down. This means that the people who would normally be making decisions aren't accessible. Their specific knowledge and expertise aren't available when you need them the most.

This is problematic because every crisis is simultaneously financial, ethical, legal, emotional, operational, and political. There are so many issues to address in so many areas that it's almost impossible to keep track of and take care of everything if you don't have a plan to which you can refer.

SOME INDUSTRIES *REQUIRE* THEM

In some industries—such as banking, financial services, hospitals, and utilities—a BCP is required by one or more regulatory agencies. Certain important federal regulations, such as the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act, contain provisions requiring companies to have a BCP to protect corporate records and confidential information.

If you're in a regulated industry, you should immediately check with your regulatory agencies to determine whether they require a BCP. If they do, your next step is to figure out the minimum requirements and start there. If you don't have a BCP, you may risk harsh penalties for noncompliance.

YOUR REPUTATION AND VALUE ARE AT STAKE

Another reason to establish a BCP is that it takes *years* for an organization to develop a solid reputation and brand. That being said, it only takes one single minor event to permanently ruin your reputation and brand. Thus, a poor response to a disaster is enough to permanently tarnish your reputation and severely impact your value.

For example, in 1997 and 1998, Nike came under great scrutiny after several reports were published about its use of child labor in the production of its clothing. The result? In a 19-month period, Nike's stock price dropped by 64 percent.

BP suffered a similar experience after the April 2010 Gulf of Mexico oil spill caused by the explosion of a rig they chartered. Though the company *did* have a disaster recovery plan, that plan was 10 years old. Worse yet, it was copied from a plan for an Alaskan rig.

Contact information was included for experts who no longer worked for the company, some were even deceased. Although the plan included steps to address sea life, that particular sea life didn't exist in the gulf.

Their unpreparedness was evident for all to see, especially when answers given by BP officials on televised press conferences were vague and unclear. Their stock suffered financially as a result.

In the year prior to the spill, BP's stock price had been steadily climbing from $40.13 to $59.88 per share, which is where it was on April 21, the day of the spill. By June 21, just 60 days later, it had dropped by 55 percent to $27.02. In a mere two months, BP had lost $103 *billion* in value.

ADDITIONAL REASONS

In addition to the above (as if they aren't enough), other reasons for creating a BCP include:

- Protecting employees and customers
- Decreasing potential exposure
- Reducing reliance on key individuals or suppliers
- Minimizing insurance premiums
- Reducing the probability of occurrence
- Protection of assets

- Minimizing exposure to civil and criminal liability
- Faster notification of an impending disaster
- More thorough approach to disaster prevention
- Faster, more immediate response
- Fewer injuries and loss of life
- Less damage to facilities and equipment
- Adequate supplies on hand
- Appropriate insurance coverage
- Increased confidence in the organization by employees *and* customers
- Ability to continue delivering goods and services
- Improved supply chain security
- Reduced cost of disaster response
- Increased value due to resiliency
- More security (aka your ability to sleep at night)
- Protection of confidential data and corporate reputation

FEMA estimates that 40 to 60 percent of all businesses never reopen after a disaster.[9] In fact, one study conducted by the University of Texas Center for Research on Information Systems found that after suffering a catastrophic data loss, *43 percent* of companies never reopen and *51 percent* close within two years.[10] Regardless of whether the number is 40 percent, 43 percent, or even 25 percent, the question *you* need to concentrate on is whether *your* company can survive!

WHY BUSINESSES FAIL TO PLAN

According to a 2016 study by Nationwide Insurance[11] a surprising 68 percent of respondents did not have a formal disaster recovery plan or BCP. In addition to not having a plan, 71 percent do not carry business interruption insurance. With so many reasons a business needs a BCP, why are there so many that don't have them?

The primary reasons given for failing to have a formal plan were:

- "I've never had an issue before/disasters are rare in my area" (41 percent).
- "I haven't really thought about it" (33 percent).
- "I don't think it's important for my business" (32 percent).
- "I've thought about it, but don't have time to come up with anything" (13 percent).

Another study—this one conducted by the business continuity information website Continuity Central[12]—asked business continuity professionals about the challenges they face with business continuity planning. The top issues cited were lack of budget, funds, and resources (38 percent), lack of top management commitment (16 percent), and staffing difficulties (6 percent).

Although you may have these issues, too, just imagine what will happen to your company if you *don't* have a plan. Isn't that much worse than facing these obstacles now, when you have maximum resources at your disposal and aren't faced with the chaos of a crisis situation?

Questions to Ask Yourself

1. List all the ways a disaster could affect your organization financially.
2. How might it benefit from having a business continuity plan?
3. Are there any regulations that require that you have a plan?
4. Superstorm Sandy hit the East Coast in late October 2012, knocking out power in many areas for more than six weeks. How would you run your organization without power?
5. Hurricane Katrina hit New Orleans in 2005 and displaced tens of thousands of people. While some organizations in the area were able to reopen, their employees had no homes to return to. How would you run your organization without employees?
6. As in the case of the small Maryland bridge that collapsed unexpectedly, if something happened in your area and your customers couldn't get to you, how would you run your organization?

7. A water bottling company purchased 20 tanker loads of spring water from a single Pennsylvania supplier. Over a weekend, the spring became contaminated and couldn't be used for drinking water. It took the bottler three weeks to find an alternate source. How would you run your organization without a key supplier?

NOTES

1. World Health Organization, Natural Events, www.who.int/environmental_health_emergencies/natural_events/en/.
2. "Disasters Affected 8% of U.S. Population in 2017, FEMA Notes in Review of Historic Year," *Insurance Journal* (January 3, 2018).
3. "Natural Disasters in 2017: Lower Mortality, Higher Cost," March 2018, Center for Research on Epidemiology of Disasters (March 2018).
4. "Natural Disasters Were Rampant in 2013," Gerald LeBlond, redOrbit.com (January 9, 2014).
5. "Oklahoma Rattled by an Uptick in Earthquakes," Laura Petrecca, *USA TODAY* (April 12, 2014).
6. "7 Everyday Ways You Are Ruining Your IQ," India Sturgis, *The Telegraph* (July 30, 2015).
7. Hurricane Michael Was the Third Most Intense Continental U.S. Landfall on Record, an Unprecedented Location for a Category 4 Landfall," Jonathan Erdman, The Weather Channel (October 9, 2018).
8. "The 15 Most Expensive U.S. Natural Disasters since 1980," Shannon McNay Insler, MSN.com (September 14, 2018).
9. "Protecting Your Businesses." Federal Emergency Management Agency (last updated September 2, 2015), www.fema.gov/protecting-your-businesses.
10. University of Texas Center for Research on Information Systems, as cited in "Impact on U.S. Small Business of Natural and Man-made Disasters" (2007), Hewlett Packard Development Company, L.P.
11. "Nationwide Survey Reveals Small-business Owners Lack a Disaster Recovery Plan," Denny Jacob, Property Casualty 360 (March 14, 2017).
12. "Business Continuity in 2014." Continuity Central (January 2, 2014), www.continuitycentral.com/feature1135.html.

CHAPTER 3

Business Continuity Planning

"Disaster recovery" is traditional terminology from the 1990s, and disaster recovery plans (DRPs) created during that time typically addressed major events, such as hurricanes, tornadoes, or earthquakes. However, not all disasters are environmental- or nature-based.

That's why, in the early 2000s, when most organizations began to rely heavily on computers, disaster recovery planning began to focus on information technology (IT) disasters. DRPs now needed to include what to do in situations such as an organization's servers going down.

Many organizations focused mainly on data recovery, but an organization does not run solely on data. Although it certainly needs access to its IT systems and data, leadership also needs to take a holistic view of the organization to better recover and address the effects on all departments and in all facets of operations.

Today's DRPs must encompass a variety of potential scenarios. After all, a terrorist attack—such as those that occurred on September 11, 2001—can be every bit as devastating as a tornado.

Two years of road construction can force a retail operation into bankruptcy. Software malfunctions and data loss from a computer virus may give a company a big enough black eye that it can never recover.

In today's complicated business environment, organizations need to consider a much broader range of disaster-related events rather than relying on the narrow focus of the traditional plans. They also need to create a more comprehensive business continuity plan.

Business continuity planning is so much more than coping with a disaster or crisis management. It's also an ongoing process that helps companies improve their chances of long-term survival by developing a comprehensive and effective response plan for dealing with unplanned interruptions to business operations.

According to the *Disaster Recovery Journal*, a business continuity plan (BCP) is "a comprehensive statement of consistent actions to be taken before, during, and after a disaster."[1] It involves disaster preparations, as well as recovery focused toward critical business operations and resumption of normal functioning in the event a disaster occurs.

This type of plan improves an organization's chances of survival. It essentially changes the disaster response from a panicked and reactive "What do we do now?" to a calm and proactive "Here is a step-by-step guide to who is going to do what and when."

The BCP also answers the following questions:

- What threats could have a severe negative impact on our operations or our brand?
- What can we do to reduce the potential impact ahead of time?
- How do we reduce potential damage *before* the event?
- How do we stop the damage from increasing in the aftermath?
- What parts of our operations need to be returned to service first?
- Who will be responsible for each part of the recovery?

To help you answer questions like these, it's important to keep in mind the business continuity cycle.

THE FIVE-STEP BUSINESS CONTINUITY CYCLE

The business continuity cycle has five steps, beginning and ending with normal operations. To help visualize the process, let's use the analogy of a person driving a car.

Step 1: Normal Operations. A person is driving the car down the highway and everything is fine.

Step 2: Disaster Event. The driver is involved in an accident, but we don't yet know the seriousness. Perhaps the car only has slight body damage and the driver is fine. While this is unpleasant and will take time to file a claim and get the car repaired, the car is still drivable. Thus, there's a minor interruption, but no major changes in the driver's activities.

Step 3: Business Disruption. As it turns out, the car is severely damaged and the driver is seriously injured, unable to function normally and can't survive without assistance.

Step 4: Emergency Response. The driver is taken to the emergency room. Doctors and nurses assess the extent of his injuries and determine how to stabilize him.

Step 5: Business Continuity. This is the period of time the driver will spend on mending his injuries.

Note that it isn't until the final step when the BCP really begins. In this step, normal operations are replaced by the BCP to allow function at some level, helping the organization maneuver through the steps necessary to return to its standard business operations. The process can be seen in Figure 3.1.

The main objective of a BCP is to protect the organization and its people, assets, and data. A *good* BCP addresses all of the critical operations and is more concerned with the effect on the functions and processes than with a specific event.

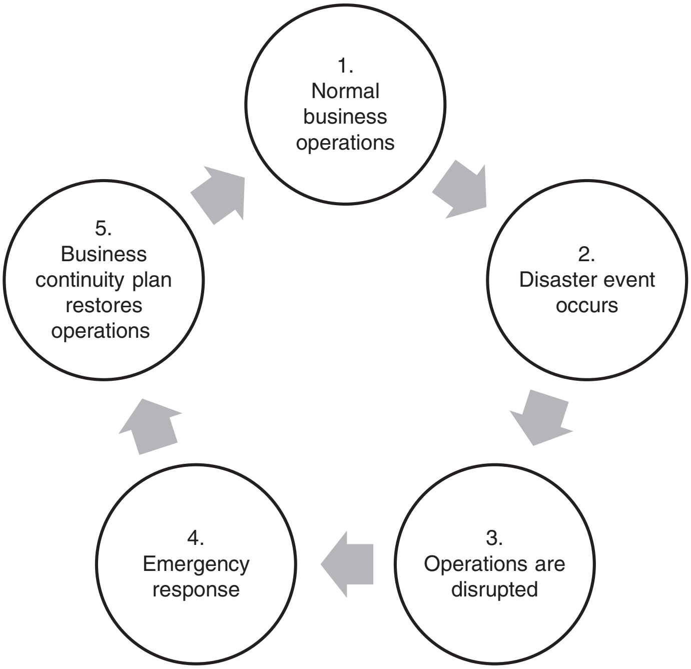


Figure 3.1 Business Continuity Cycle

For instance, how you cope without power for a month is more important than whether the outage was due to a hurricane, tornado, or earthquake.

The BCP should also:

- Mitigate damage
- Minimize extent and duration of disrupted operations
- Provide a sense of stability
- Reduce decision making in the middle of the disaster

So, what's the process for creating a comprehensive, disaster-worthy BCP? I thought you'd never ask.

THE BUSINESS CONTINUITY PLANNING PROCESS

As with any major initiative, successful business continuity planning requires an understanding of the overall process, the desired goals and outcomes, and the critical elements for success.

As we saw earlier, the business continuity cycle goes like this:

Step 1: Normal business operations

Step 2: Disaster event occurs

Step 3: Operations are disrupted

Step 4: Emergency response

Step 5: BCP restores operations

Again, the BCP does not start until Step 5. But, if no BCP is in place, affected organizations may not react quickly enough to survive. And even if they *do* survive, their brand and reputation may be permanently tarnished from a poor disaster response.

Business continuity planning can be broken down to a 10-step process. These steps will make up the remainder of this book but, briefly, they are:

Step 1: Obtain Management Support. For business continuity planning to succeed, it must get the full (and visible) support of management.

Step 2: Assemble a Planning Team. The business continuity planning team must address all major functional areas of the organization and include members from all levels of responsibility.

Step 3: Collect Data. A lot of data needs to be collected before the planning process begins, including information about current operations, employees, vendors, customers, and insurance policies.

Step 4: Evaluate Operations. Each area of the organization needs to be evaluated for both strengths and weaknesses. You must understand the mission-critical processes and where they could break down.

Step 5: Identify and Evaluate Risks. This step involves identifying all of the threats that might impact your organization's operations, followed by an evaluation of impact to rank each one by overall impact.

Step 6: Determine Recovery Strategies. Different threats involve different recovery strategies. These strategies can range from prevention to insurance to mitigation.

Step 7: Organize and Document a Written Plan. The written document becomes a step-by-step "how-to" manual for responding to disaster situations.

Step 8: Communicate the Plan. The best plan is useless unless it is communicated properly to all affected individuals.

Step 9: Test the Plan. You can never be sure about the effectiveness of your plan until you test it. Testing can range from a small table-top exercise to a live simulation involving the entire community.

Step 10: Evaluate and Update the Plan. The BCP is not a "one-and-done" exercise. It must be continually evaluated and updated.

GETTING STARTED

Business continuity planning can be a difficult process to get started. It is time-consuming and uses valuable resources (even though the best outcome is never having to use it). No wonder so many businesses don't take the time to create one!

But all it takes is one minor disaster to show you just how important having a plan can be. Executives usually aren't very happy when the entire organization is unproductive. If the power goes out for an hour, for example, the 60 minutes of downtime can easily turn into thousands of dollars of expense.

To start the process off on solid footing, it's important to be very clear about the benefits of disaster planning, some of which we've already covered. This is necessary because it can really help you gain management support and resources, which is step one and what we're going to focus on next.

Questions to Ask Yourself

1. What processes do you already have in place to protect your organization?
2. How might a BCP make these protections even stronger?
3. Of the 10 steps in the BCP process, which ones do you see as the biggest obstacles?
4. Which ones are likely to have the least resistance?

NOTE

[1] "Disaster Recovery Planning Process, Part I," Geoffrey H. Wold, *Disaster Recovery Journal* 31, no. 4 (Winter 2018).

CHAPTER 4

Step 1: Obtain Management Support

Any major initiative in an organization needs management support. Without it, it becomes just another project that was started but faded away into obscurity.

That's why business continuity needs to be approached from the position that it is an essential part of a strategy that helps the company achieve its mission and vision. Because every organization needs to generate revenue to achieve the goals it set out to accomplish, ensuring success requires that the individuals within the organization understand what could cripple this process. They realize that they must have a plan to minimize the impact of a disaster. In effect, a business continuity plan (BCP) is a life insurance policy for the organization!

When you can get management on board, offering strong support for the creation of a BCP, benefits include access to resources and funding and support from all levels of the organization. This can make all of the difference in the world. But why is management so important?

MANAGEMENT'S ROLE

Management has several roles in the business continuity process. Although it doesn't need to be intimately involved with every aspect, members of the management team have critical responsibilities that can make or break the success of a BCP.

First and foremost, managers need to communicate their support to everyone in the organization. They have to be able to explain *why* the process is so important to the overall achievement of the company's mission.

This can help each department better understand how the BCP will enable them to operate with some level of effectiveness in the case of an emergency or disaster. If executed correctly, it will also enable each employee to understand that a good BCP can help them keep their job.

Second, management should be responsible for identifying the critical functions of the organization. In a disaster, not all parts of the company can get back up and running immediately. Thus, management team members should determine which functions must be operational as soon as possible, prioritizing them and specifying the order of focus.

In addition to supporting the process, management should also be responsible for the oversight and coordination of the plan. This means following up on the progress of plan development to ensure that it's completed in a timely manner.

A final responsibility of management involves the overall effectiveness of the plan. Management should look at the plan from the big-picture perspective of the organization, evaluating whether all critical systems have been addressed and in the appropriate order. This means asking the question, "If this doesn't work, what would we do instead?"

Management's ultimate responsibility is to ensure that the business achieves its mission. *Thus, management's responsibility to business continuity planning is to ensure that nothing gets in the way of that goal.*

OBTAINING MANAGEMENT SUPPORT AND APPROVAL

Management teams tend to have competing priorities, which means that it's not always easy getting their attention for business continuity planning. Often, this type of planning is seen as an unnecessary cost. After all, it doesn't generate revenue and the best outcome possible is to never even use it!

When presenting the idea for a BCP, it's important to approach it from the perspective of the C-suite, which refers to the company executives who are in the highest-level positions (think: CFO, CEO, and COO). Address their top question, their WIIFM, or *What's in it for me?*

This requires understanding what's important to them and how a BCP would impact them directly. Therefore, for each executive, consider where he or she may be coming from. What are his or her areas of responsibility? What is he or she most concerned about?

Understanding executives' individual needs and worries can help you frame your message so it is relevant and applicable to *them.* The BCP can then be presented as a solution to *their* particular concerns and issues.

Also consider how they might respond. There are two distinctly different responses to continuity planning depending on the person's previous experience and attitudes toward risk. To determine which one is most likely, ask yourself: Is this executive generally risk averse? Do they always have a “Plan B”? If so, they are likely already on your side and will require very little convincing.

However, some executives love risk and assume that everything will always work out. Or, they may have never thought about continuity planning because they don’t think a disaster is likely to happen to them. For them, you need to sharpen your story and be very clear.

Be prepared for a negative response and possible misconceptions and consider how you can respond to their concerns without getting defensive. Focus on how the BCP can help them protect everything they’ve worked so hard to build.

Consider also delivering a story about a disaster *you* experienced or a “near-disaster” that created chaos at a previous organization. Often, when trying to convince people of the merits of a project, they may not relate to high-level explanations but can relate to a story.

If you don’t have a specific event that occurred at your company, tell them about an event that occurred at a similar company. Describe how it affected operations, how it was handled, how visible it was to customers and the public, and the end result.

Quantify the impact in lost revenue, lost work hours, additional costs, bad public relations, fines, and lawsuits (*no bonuses*). Follow up with a discussion of how a BCP could have improved the situation.

Another option is to provide articles describing the effects of nearby disasters. One great one was published in May 2013 in the *Journal of Accountancy*. It was titled “Preparing for Disaster” and focused on CPAs who survived Hurricane Katrina, Superstorm Sandy, and the tornadoes that struck Joplin, Missouri.

Reading accounts of disaster-impact from the executives who went through those experiences really brings home the need for continuity planning. For instance, Jim Hardy, founder of Hardy, Wrestler, and Associates, saw his company’s 20-person office flattened by a tornado in a matter of seconds. In the article, he says, “The biggest thing I can’t stress enough . . . is to have a disaster plan so you know what your steps are immediately following the disaster.”[1]

In addition to understanding the perspective of each executive, be clear about what you want to achieve. Are you trying to increase awareness and educate? Are you looking for support and approval for the project? Do you want funding or other resources? Having clearly defined goals will help you deliver the right message to management and with the appropriate context.

In many cases, it's easier to pitch the creation of a BCP to executives individually before asking the C-suite to vote on the proposal. This may be more time-consuming, but along the way you might find one executive who buys in completely and can become your BCP champion. This can open many doors and ease the way to approval.

The chart in Figure 4.1 can be used to evaluate your management's views toward risk and business continuity planning. Use the following process to complete the chart:

Step 1: In column 1, list each member of your management team.

In column 2, indicate whether you believe they are risk averse. (Do they like surprises? Always have a backup plan?) Write a Y for yes, N for no, or a question mark if you're not sure.

In column 3, list the person's areas of responsibility (sales, HR, IT, etc.).

In column 4, list any of their individual concerns. (What keeps them awake at night? What are they afraid of?)

(1)	**(2)**	**(3)**	**(4)**	**(5)**
Name or Title	**Risk Averse? (Y, N, or ?)**	**Areas of Responsibility**	**Concerns or Fears**	**Departmental Vulnerabilities**

Figure 4.1 Evaluation of Management's Approach to Risk

In column 5, give your perspective on their departmental weaknesses or vulnerabilities.

Step 2: Based on this chart, how supportive do you think your management team will be toward business continuity planning?

Questions to Ask Yourself

1. In order to get the support of your management team, what examples, events, or stories could you use to get their attention?
2. What was the impact of each event?
3. How could a BCP have improved the response or decreased the loss?

NOTE

1. "Preparing for Disaster," Jeff Drew and Ken Tysiac, *Journal of Accountancy* (May 2013).

CHAPTER 5

Step 2: Assemble a Planning Team

The second step to business continuity planning requires that you have a comprehensive and detailed understanding of both the big picture and day-to-day company operations. This level of understanding is difficult to find in just one individual, which is why this step involves assembling a planning team.

The benefits of using a team approach include:

- Increased visibility of the process
- Representation from each area of the organization
- More investment and buy-in
- Spreading of the workload
- Different perspectives
- Greater discussion
- Increased quality in problem solving

ROLE OF THE PLANNING TEAM

The role of the business continuity planning team begins with development, documentation, and implementation of the plan in a timely manner.

The team also needs to ensure that the plan addresses all critical functions of the organization and meets the desired recovery objectives.

The planning team will determine the scope of the plan and the criteria for its success. Team members will be assigned responsibilities for later steps, such as collecting data, developing alternate response options, and writing the document.

The planning team should also be responsible for:

- Detecting and announcing disaster events
- Initiating disaster recovery response
- Activating the business continuity plan (BCP)
- Monitoring the situation until operations return to normal
- Deactivating the business continuity procedures once this occurs
- Testing the procedures and regularly updating and improving the plan

WHO TO INCLUDE

The size of your team will depend on the size and complexity of your organization. Regardless, because it must have a complete understanding of the business and its functions, your team should include members from each of the departments of your organization whenever possible.

You may also consider including key customers and suppliers as part of the team. They not only bring a much different perspective to the process but may also be crucial to your successful return to normal operations. Plus, if a vendor has been involved in developing your BCP, you will likely be higher on their list of companies to respond to should a disaster occur.

Including key customers means they'll likely be far more understanding of any delays or disruptions to their service should a disaster occur. Depending on the size of your organization, the nature of your business, or its reach into the community, you may also consider involving the Red Cross (or representatives of your local or state governments).

Another important factor in developing your team is to include members from all levels of the organization, from upper management down to the rank and file. Each level has a different perspective, and participation will increase their buy-in on the final plan.

When it comes to specific members of the team, one key member would be the chief operating officer (COO). COOs have the greatest understanding of the overall operations of the organization. Other key members from finance, IT, HR, facilities/maintenance, health and safety (if separate from HR), security, community relations, legal, purchasing, and labor representatives should be also consulted.

Figure 5.1 can be used to list the members of your team to ensure representation from each department and all levels of authority.

ORGANIZATION OF THE TEAM

There's no single way to organize a planning team. However, there should be clear lines of authority, reporting, and decision making within it. Roles and responsibilities should be clearly defined during

Name and Title	Department	Level (Executive, Management, or Staff)	Responsibilities

Figure 5.1 Members of Your Planning Team

the BCP development process, as well as during an emergency. The team should also include a primary and a backup leader during a crisis.

While establishing these levels of authority and responsibility, strive to allow for the free flow of information. All members should feel comfortable with contributing their observations, questions, and concerns, regardless of their level of responsibility.

You can choose to involve each member in the entire process or you can assign specific roles, such as:

- **Emergency Response.** This person would be responsible for health and safety considerations, damage assessment, damage mitigation, and immediate repairs should a disaster occur.
- **Internal and External Communications.** Someone in this position would handle both employee communications and public relations.
- **Vendor Management.** The individual in this role would be responsible for identifying key suppliers and finding alternate sourcing.
- **Customer Relations.** The person in charge of customer relations would identify key customers and establish minimum performance levels.

- **Computer Services.** The customer service role would handle all aspects of the business associated with data integrity and alternate access options.
- **Community Interaction.** Someone filling this position would coordinate response efforts with local fire and police, FEMA, and all available aid organizations.

THE FIRST MEETING

Success in the first planning team meeting is crucial to the ultimate success of the BCP. Therefore, it needs to address the purpose of the BCP. Each member must have a clear understanding of the specific goals.

You might even consider having the team develop a mission statement to demonstrate the organization's understanding and commitment to business continuity. By reviewing the mission statement on a regular basis (especially when making key decisions), management can keep everyone focused.

Second, use this very first meeting to review the 10 steps to the planning process. Identify the roles each member will take and assign the responsibilities appropriately.

Finally, establish a tentative timeline and a budget. The timeline can be amended as the process becomes more defined (or priorities change). Establishing a budget ensures that the appropriate resources will be available. Additionally, when management signs off on the budge it will demonstrate their support for the process, which is *huge.*

Questions to Ask Yourself

1. Who will you include on your planning team? (Be sure to include someone from each department.)
2. Who will lead the team?
3. How will you organize the team? Will you assign specific roles?
4. When will you hold your first meeting?
5. What will include on the agenda for your first meeting?

CHAPTER 6

Step 3: Collect Data

You need to understand the overall operations of your organization, the specific operations of each department, and the functions necessary for each department to operate in order for your business continuity plan (BCP) to be effective. That's why the third step involves collecting information.

When collecting data, consider the following questions:

- What are your main products or services (in volume and in financial value)?
- How do you produce or deliver them?
- Who would be affected if you were prevented from delivering as scheduled?
- What legal, contractual, regulatory, and financial obligations do you have?
- What functions could be performed at an alternate location?
- What functions, if you were not able to perform them, would be an inconvenience as opposed to a disaster?
- What functions are performed on a daily basis?
- What functions have reasonable workarounds?
- What vendors do you rely on (sole suppliers, payroll processing, billing) during the normal course of business?

IDENTIFY YOUR MISSION-CRITICAL FUNCTIONS

Your next step is to identify and list your mission-critical functions. What are these?

A mission-critical function is any function that *must* continue to occur, even without access to the normal equipment, data, facilities, or staff. For instance, consider the products and services you provide. What resources do you need to produce or provide them? Do you have any significant or sole source suppliers?

Additionally, what personnel are critical to these functions? (Hint: It's not always management!) Think also about what services are critical. Consider your needs regarding electricity, gas, water, sewer, telephone, Internet, and transportation.

Once these mission-critical functions are identified, prioritize and rank them in order of importance. Resources you rely on the most must be tended to first, with all of the remaining needs falling where they should be in line.

DEPARTMENT EVALUATIONS

Next, evaluate each department for functions, key personnel, data and information, processing, hardware and software systems, equipment, safety, interaction with others (departments, customers, and vendors), documentation, policies and procedures, and external regulations.

Use of a form, such as the one shown in Figure 6.1, is helpful in analyzing each of these areas.

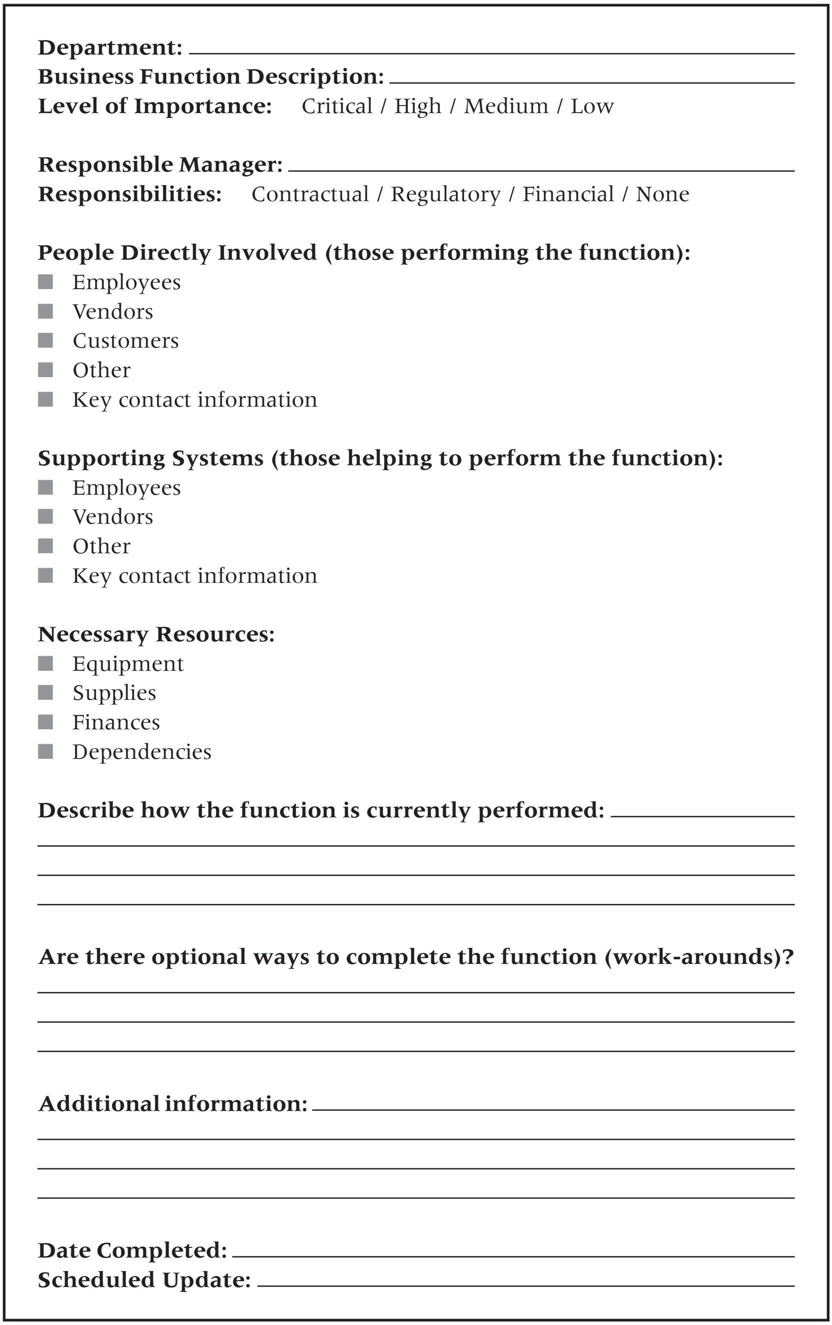
POLICIES AND PROCEDURES

Data collection also includes identifying the policies and procedures you *already* have in place that might help with business continuity, ensuring that each one is up-to-date, accurate, and reflects actual operations. Consider your:

- Evacuation plans
- Fire protection plans
- Health and safety programs
- Environmental policies
- Security procedures
- Purchasing procedures
- Facility closing policies
- Employee manuals
- Hazardous materials plans

Next, identify the insurance coverage you currently have. (*Appendix A contains a sample worksheet you can use to record all of your current insurances.*) When compiling your list, pay special attention to what is *not* covered as well. This is also a good time to look at current deductibles and gain a better understanding of what conditions may increase them.

Insurance is discussed at greater length in later chapters. However, to begin, at least collect and document whatever information you can about your particular policies.



Department: ______________________________

Business Function Description: ______________________

Level of Importance: Critical / High / Medium / Low

Responsible Manager: __________________________

Responsibilities: Contractual / Regulatory / Financial / None

People Directly Involved (those performing the function):

- Employees
- Vendors
- Customers
- Other
- Key contact information

Supporting Systems (those helping to perform the function):

- Employees
- Vendors
- Other
- Key contact information

Necessary Resources:

- Equipment
- Supplies
- Finances
- Dependencies

Describe how the function is currently performed: __________

____

____

____

Are there optional ways to complete the function (work-arounds)?

____

____

____

Additional information: ___________________________

____

____

____

Date Completed: ____________________________

Scheduled Update: ___________________________

Figure 6.1 Business Function Summary Form

REGULATORY CODES AND REQUIREMENTS

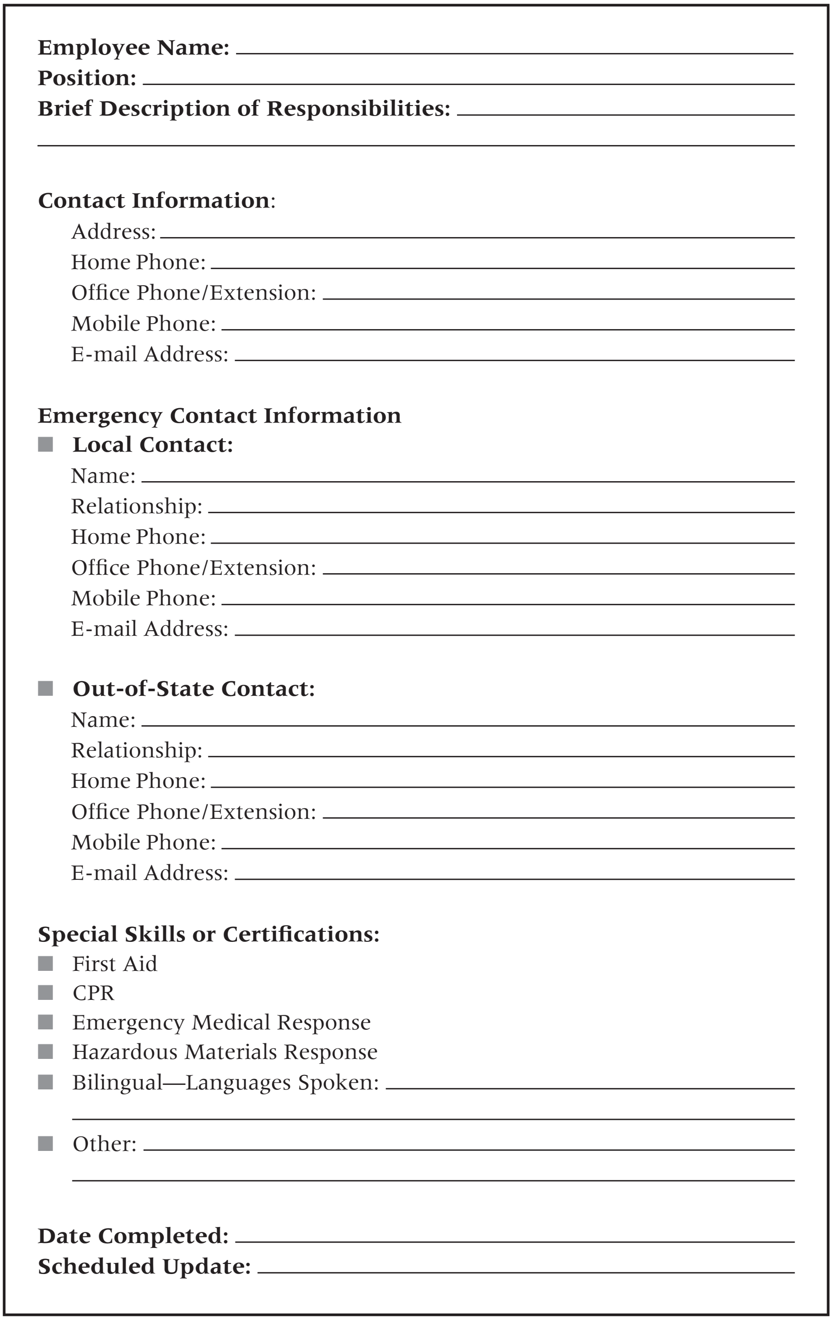
As mentioned previously, some industries have regulations in place regarding what needs to be in your BCP. Review those now so you know what your business is subject to at the local, state, and federal levels. Don't make a disaster worse by violating applicable statutes.

Consider regulations and restrictions related to occupational health and safety, environmental regulations, fire codes, transportation codes, zoning regulations, Sarbanes-Oxley, and HIPAA (Health Insurance Portability and Accountability Act).

USEFUL DOCUMENTS

As part of the data collection process, there are many other documents that are useful to have available. These include:

- Insurance policies
- Banking information
- Finance information
- Critical phone numbers
- Employee contact information
- IT inventory (software, hardware, and data)
- Master vendor list
- Equipment inventory
- Temporary location information
- Remote access instructions
- Key usernames and passwords
- Building owners or managers
- Utility providers
- Telephone and Internet providers
- Professional contacts (CPA, lawyer, insurance agent, bank)
- Notification checklist



Employee Name: ______________________________

Position: ______________________________

Brief Description of Responsibilities: ______________________________

____

Contact Information:

Address: ______________________________
Home Phone: ______________________________
Office Phone/Extension: ______________________________
Mobile Phone: ______________________________
E-mail Address: ______________________________

Emergency Contact Information

■ **Local Contact:**

Name: ______________________________
Relationship: ______________________________
Home Phone: ______________________________
Office Phone/Extension: ______________________________
Mobile Phone: ______________________________
E-mail Address: ______________________________

■ **Out-of-State Contact:**

Name: ______________________________
Relationship: ______________________________
Home Phone: ______________________________
Office Phone/Extension: ______________________________
Mobile Phone: ______________________________
E-mail Address: ______________________________

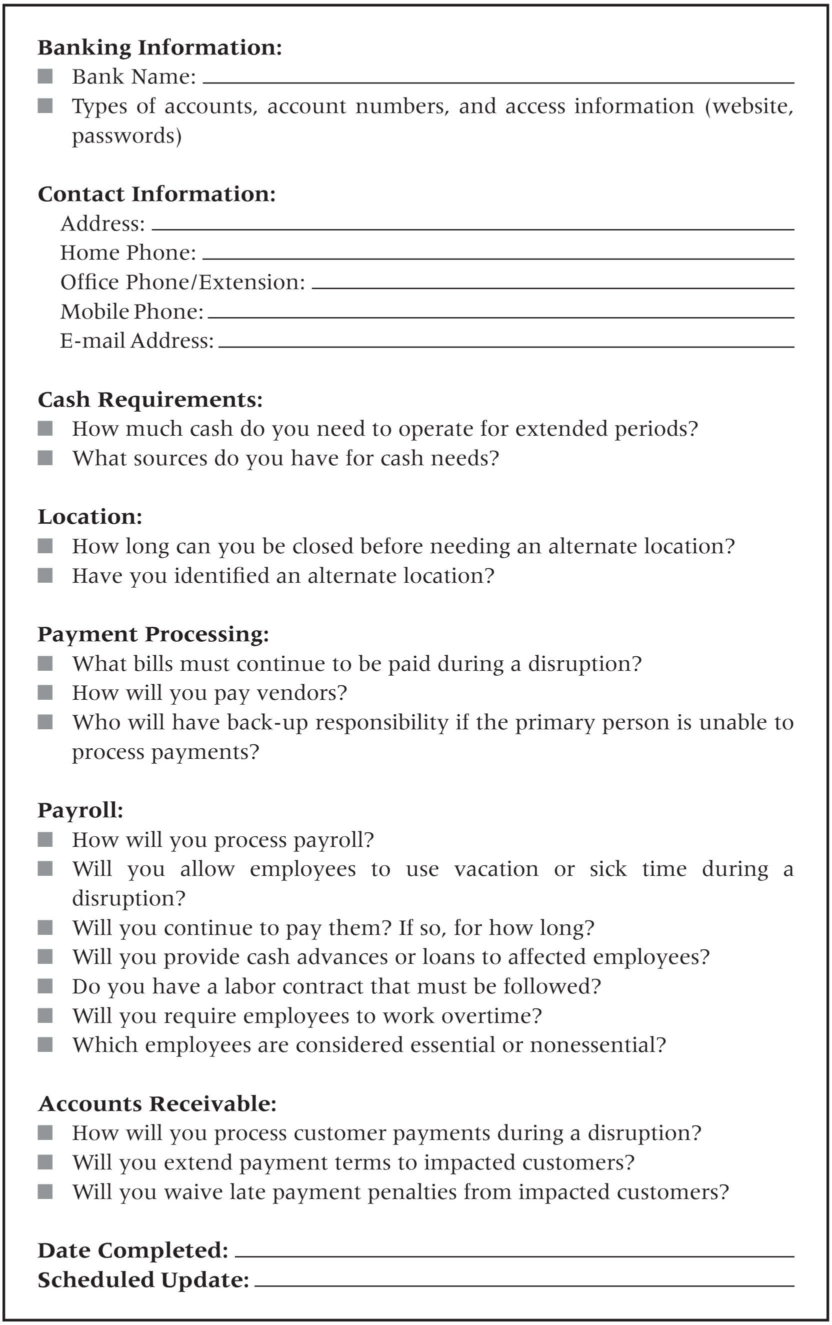
Special Skills or Certifications:

■ First Aid
■ CPR
■ Emergency Medical Response
■ Hazardous Materials Response
■ Bilingual—Languages Spoken: ______________________________
____
■ Other: ______________________________
____

Date Completed: ______________________________

Scheduled Update: ______________________________

Figure 6.2 Employee Information Form



Banking Information:

- Bank Name: ______________________________
- Types of accounts, account numbers, and access information (website, passwords)

Contact Information:

Address: ______________________________
Home Phone: ______________________________
Office Phone/Extension: ______________________________
Mobile Phone: ______________________________
E-mail Address: ______________________________

Cash Requirements:

- How much cash do you need to operate for extended periods?
- What sources do you have for cash needs?

Location:

- How long can you be closed before needing an alternate location?
- Have you identified an alternate location?

Payment Processing:

- What bills must continue to be paid during a disruption?
- How will you pay vendors?
- Who will have back-up responsibility if the primary person is unable to process payments?

Payroll:

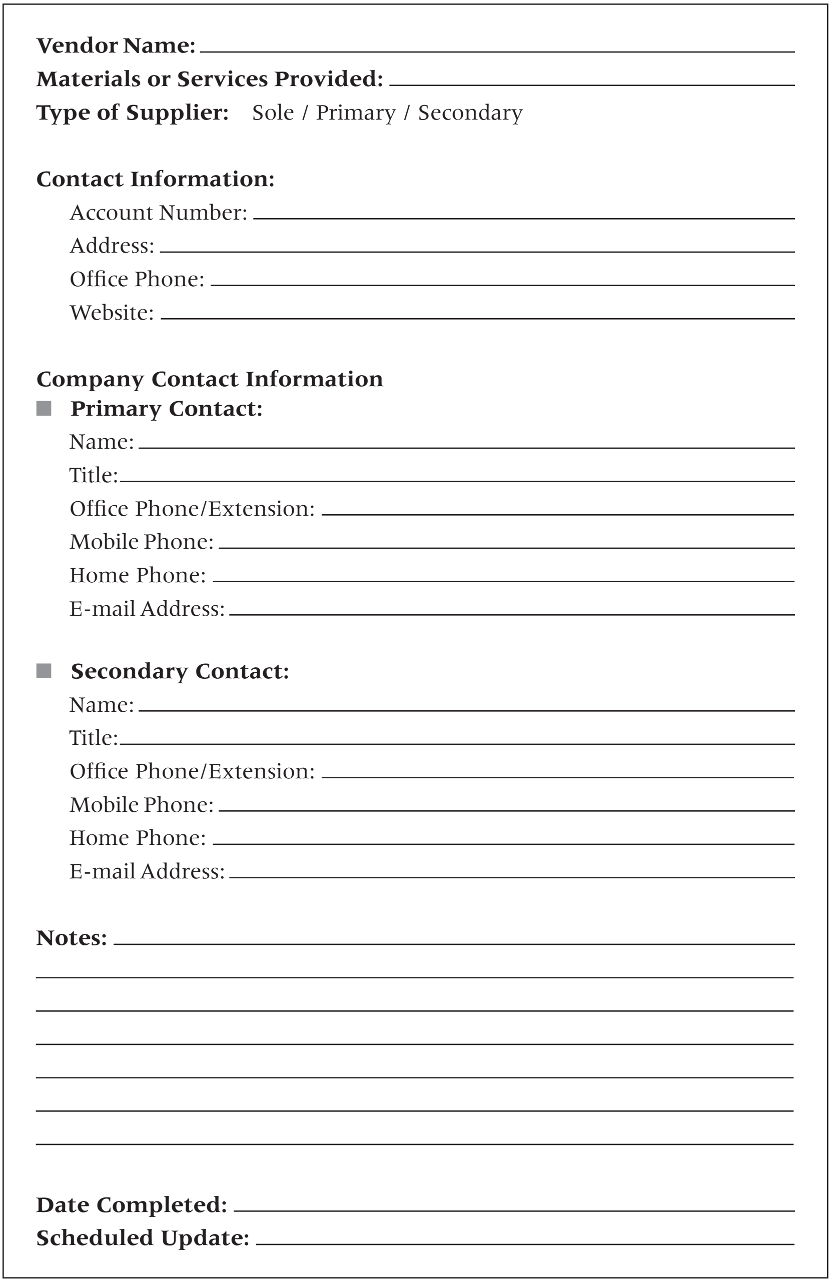
- How will you process payroll?
- Will you allow employees to use vacation or sick time during a disruption?
- Will you continue to pay them? If so, for how long?
- Will you provide cash advances or loans to affected employees?
- Do you have a labor contract that must be followed?
- Will you require employees to work overtime?
- Which employees are considered essential or nonessential?

Accounts Receivable:

- How will you process customer payments during a disruption?
- Will you extend payment terms to impacted customers?
- Will you waive late payment penalties from impacted customers?

Date Completed: ______________________________
Scheduled Update: ______________________________

Figure 6.3 Finance Information Form



Vendor Name: ______________________________

Materials or Services Provided: ______________________________

Type of Supplier: Sole / Primary / Secondary

Contact Information:

Account Number: ______________________________

Address: ______________________________

Office Phone: ______________________________

Website: ______________________________

Company Contact Information

■ **Primary Contact:**

Name: ______________________________

Title: ______________________________

Office Phone/Extension: ______________________________

Mobile Phone: ______________________________

Home Phone: ______________________________

E-mail Address: ______________________________

■ **Secondary Contact:**

Name: ______________________________

Title: ______________________________

Office Phone/Extension: ______________________________

Mobile Phone: ______________________________

Home Phone: ______________________________

E-mail Address: ______________________________

Notes: ______________________________

____

____

____

____

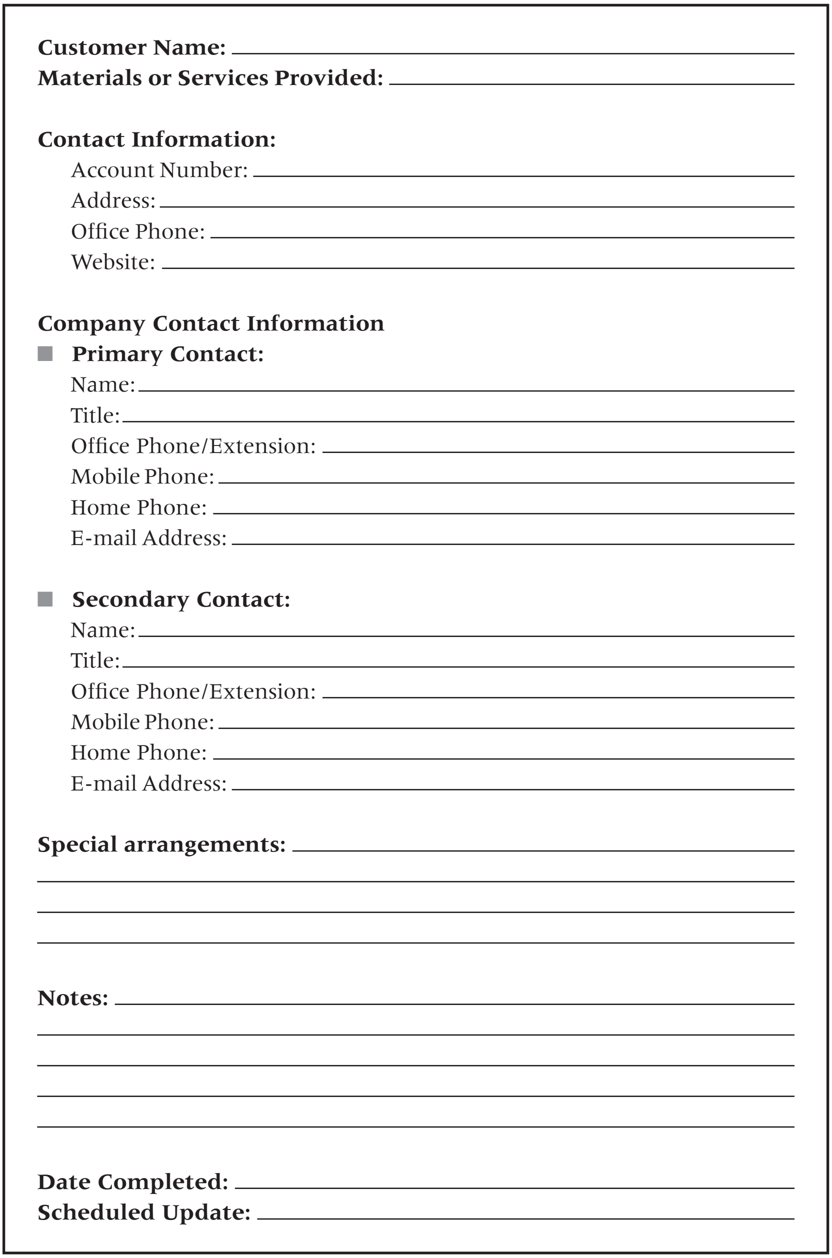
____

____

Date Completed: ______________________________

Scheduled Update: ______________________________

Figure 6.4 Vendor Information Form



Customer Name:
Materials or Services Provided:

Contact Information:
Account Number:
Address:
Office Phone:
Website:

Company Contact Information

- **Primary Contact:**

Name:
Title:
Office Phone/Extension:
Mobile Phone:
Home Phone:
E-mail Address:

- **Secondary Contact:**

Name:
Title:
Office Phone/Extension:
Mobile Phone:
Home Phone:
E-mail Address:

Special arrangements:

Notes:

Date Completed:
Scheduled Update:

Figure 6.5 Key Customer Information Form

SAMPLE FORMS

In the preceding pages are sample forms for collecting information about employees, finances, vendors, and suppliers. Each one contains the information necessary to complete your data collection process.

When creating your own forms, don't be afraid to modify them to include any additional information you may need should a disaster occur. The easier you make it on yourself and your organization in that type of situation, the more the business continuity planning process will pay off.

Questions to Ask Yourself

1. What are our mission-critical functions?
2. What policies do we have in place that can help our company in the event of a disaster?
3. Which ones don't we have that we should?
4. Are there regulatory codes and requirements we must meet with our BCP? If so, what are they?

CHAPTER 7

Step 4: Evaluate Operations

Once your data is collected, the next step is to organize it so you can evaluate your company's operations processes. This makes it easier to create your business continuity plan (BCP). One effective tool for this purpose is a flowchart.

Formal flowcharts can be prepared using software or, simply, by using nothing more than pen and paper. Regardless of the methodology, it should identify each specific process within a department. From there, you will highlight the key steps that absolutely must happen in each one to fulfill its particular functions.

Take the sales department, for example. In order to complete a sale, a critical function would be the sale initiation. After all, if the customer can't reach you, nothing further will happen.

However, if your sales software was temporarily disabled, an order might still be able to be processed. Yes, it may take a little longer, but this could still be handled by hand. Your flowchart should reflect this.

The flowchart should also identify the person or persons responsible for each function. Look for individuals who are intertwined throughout the process and ask: What would happen if they weren't available?

When evaluating your company's operations, think also of individuals outside of the corporation who are critical to the process. One example of this is outside stakeholders.

A disaster will affect more than just your company and its employees. It may also impact your customers, your vendors, your town, and your state.

Involving everyone who could be affected will increase the effectiveness of your continuity plan.

With this in mind, consider meeting with your largest customers to discuss their concerns and potential needs during a disaster. Depending on your industry, some may want to arrange special contracts for services during that time. For example, a bottled water company may establish an arrangement to provide water to critical-needs customers first, such as hospitals or nursing homes.

Also consider discussing your requirements with your most critical vendors, establishing priority arrangements with them as well. Find out what disaster plans they have in place. For sole suppliers, identify an alternate as a potential backup.

Finally, meet with profit and nonprofit organizations involved in the disaster recovery. They can provide invaluable information you may have overlooked or can use to facilitate your business continuity planning process.

Make inquiries about the types of disasters and emergencies that you are most concerned about, the plans the governmental and non-governmental agencies have in place to address those events, and available resources for both short- and long-term response.

Possible agencies or organizations to consider contacting include:

- Community Emergency Management Office
- Federal Emergency Management Agency (FEMA)
- Local fire, police, and public works departments
- The National Weather Service
- American Red Cross
- Local utilities and telephone companies
- Neighboring businesses
- Occupational Health and Safety Administration (OSHA)

Questions to Ask Yourself

1. What specific processes should my company be most concerned about?
2. What are the key steps that need to happen to complete each of your key processes?
3. Who are the people responsible for these functions?
4. What outside stakeholders could potentially be valuable when creating the BCP?

CHAPTER 8

Step 5: Identify and Evaluate Risks

The fifth step, risk management, *is about reducing the effect of uncertainty on your objectives.* That makes it an integral part of every organization's business continuity plan (BCP).

Most businesses focus on the positive steps that they can take to achieve their goals, but often overlook the negative events that can make it more difficult (or even impossible) to achieve those goals.

A common mistake many companies make is seeing this as a one-and-done event. Unfortunately, the world is a risky place (and getting riskier all the time) with new threats developing every day . . . so looking at disasters and emergencies as isolated events is a dangerously myopic mind-set.

Businesses *must* be continually vigilant so they don't get caught off guard by an unforeseen event. Thus, risk management should be an ongoing process, an integral part of the strategic planning process.

RISK ASSESSMENT PROCESS

Risk assessment is a process designed to identify and evaluate threats and hazards that could potentially harm a business. It involves considering the types of threats that exist, the assets at risk from the threats, and the potential negative impacts.

Companies that define the potential disasters and emergencies that they might encounter will have *situation awareness* at the most hazardous and critical of times. They will have focus and vision while their clueless competition flounders in chaos.

A company's assets can take many shapes and forms, and risk assessment should consider the impact on all of them. These assets may include people, data, equipment and vehicles, facilities, proprietary information, utility systems, raw materials, supplies, inventory, and even reputation.

First and foremost, an organization should always be concerned with the safety of its people. This includes employees, customers, vendors, and other stakeholders and involves creating response plans to address any threat that could cause personal injury to them.

Second, when conducting a risk assessment, you want to look for your vulnerabilities. Where are the weak links that could create the most damage? How do you address each one?

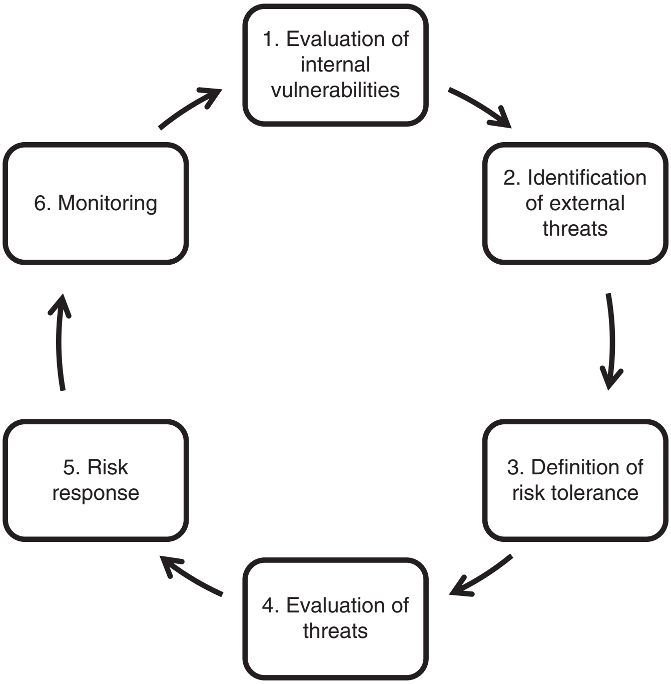

1. Evaluation of internal vulnerabilities
2. Identification of external threats
3. Definition of risk tolerance
4. Evaluation of threats
5. Risk response
6. Monitoring

Figure 8.1 Risk Assessment Process

One option is to choose to accept the risk and do nothing. Other alternatives are to avoid the risk entirely, take steps to mitigate damage, or insure against potential loss.

The risk assessment process has six steps (see Figure 8.1).

STEP 1: EVALUATION OF INTERNAL VULNERABILITIES

In this phase, you develop a thorough understanding of all of your business processes and where they might break down. This involves collecting information about your organization's current operations (which you've already done), as well as the specific operations of each department and the functions necessary for them to operate.

For this step, it's helpful to refer back to the questions posed at the beginning of step three. Look also at your mission-critical functions and your policies and procedures.

These types of exercises make it easier to see where your internal vulnerabilities may lie. In turn, adding your responses to them in your

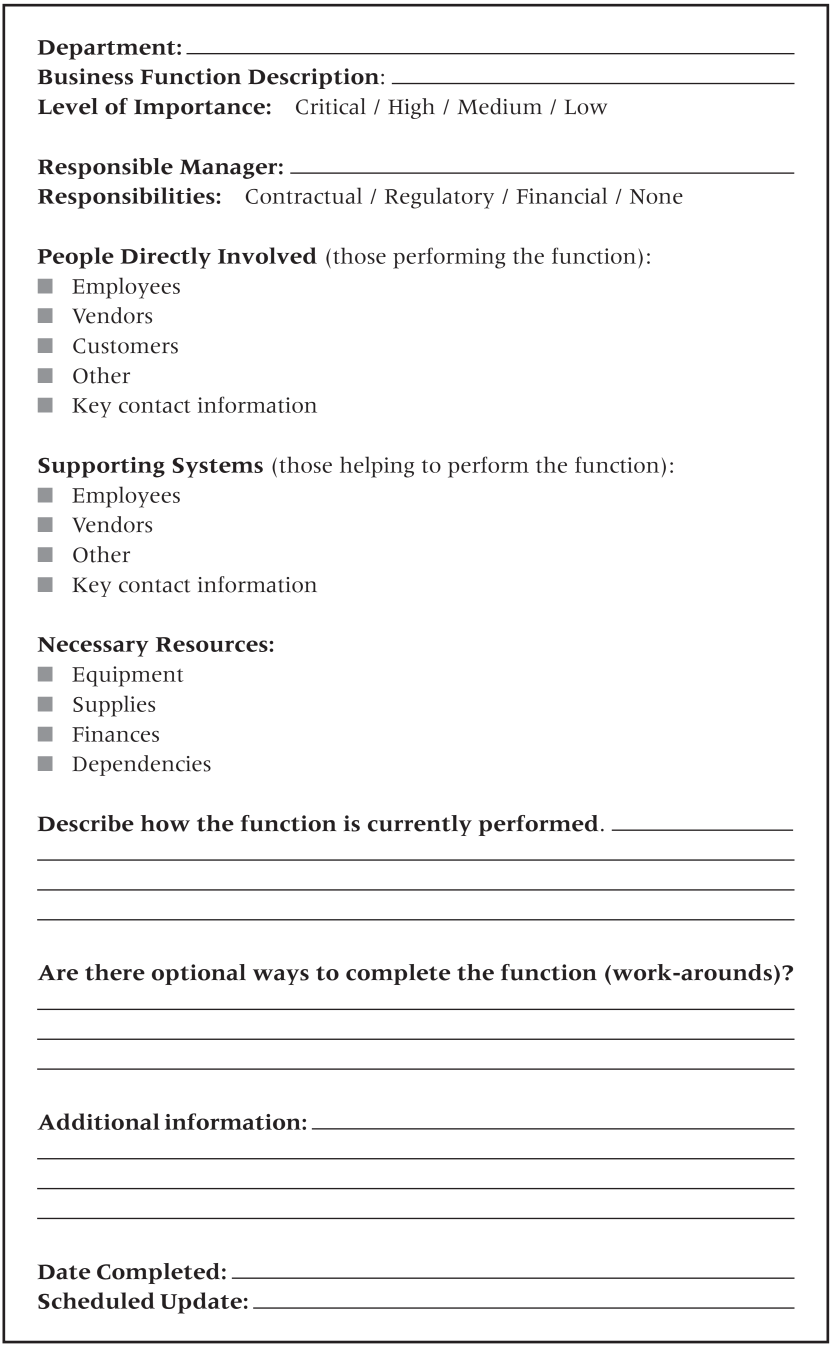
BCP can only make your business stronger if it ever finds itself face-to-face with a disaster, whether natural or man-made.

Also, a sample Business Function Summary Form (Figure 8.2) is included to help walk you through the process. Or, if you'd prefer, you can also document your procedures and their possible vulnerabilities with a simple flowchart.

An important part of risk assessment involves understanding the nature of your facilities and their vulnerabilities. This means identifying all of your major systems, their locations, and their current condition.

When considering your facilities, think about and document (preferably with photographs or videos as these will help tremendously in the event you must file an insurance claim) the following:

- **Physical Locations:** Prepare a list of each of your facilities. Include the physical address and a brief description of each. If possible, locate a floor plan, verifying that it is correct and taking special note of exit routes.
- **Exterior Grounds:** Look for dead trees, tree limbs, or loose stored materials as these can become destructive missiles in high winds.
- **Stored Materials:** Prepare a list of flammable or hazardous materials in each facility. Identify the location, type of material, typical range of quantity on hand, and its characteristics. *Get a copy of the Materials Safety Data Sheet (MSDS) for each hazardous chemical.*
- **Gas Meters and Shut-Off Valves:** If your buildings are serviced by natural gas or propane, prepare a list of each area serviced, identifying the location of both the meters and shut-off valves. Make sure the valves are serviceable, clearly marked, and easily accessible.
- **Breaker Panel:** For each facility, locate the breaker panel. Ensure they are appropriately marked, easily accessible, and that all fuses are labeled correctly.
- **Fire Extinguishers:** Locate the fire extinguishers in each facility. Make sure each one is up-to-date, is the appropriate type for your needs, and is appropriately marked and easily



Department: ____________________

Business Function Description: ____________________

Level of Importance: Critical / High / Medium / Low

Responsible Manager: ____________________

Responsibilities: Contractual / Regulatory / Financial / None

People Directly Involved (those performing the function):

- Employees
- Vendors
- Customers
- Other
- Key contact information

Supporting Systems (those helping to perform the function):

- Employees
- Vendors
- Other
- Key contact information

Necessary Resources:

- Equipment
- Supplies
- Finances
- Dependencies

Describe how the function is currently performed. ____________________

____

____

____

Are there optional ways to complete the function (work-arounds)?

____

____

____

Additional information: ____________________

____

____

____

Date Completed: ____________________

Scheduled Update: ____________________

Figure 8.2 Business Function Summary Form

accessible. Also make sure you have enough of them for the size of your facility.

- **Artwork:** Prepare a list of all artwork in your facility, such as paintings or sculptures. Include a description, location, artist, purchase date, purchase price, and current value, if known.
- **Take Photographs or Videos:** Make a note in your calendar to update them every year.

Another part of your risk assessment should involve identifying and documenting your utility systems and major equipment.

Begin by preparing a complete list of your utility systems, including:

- Heating
- Cooling
- Electric
- Natural gas
- Water
- Fire suppression
- Generators

Prepare a list of all of your major equipment, including:

- Elevators
- Manufacturing equipment
- Warehousing equipment
- Vehicles
- Telephone
- IT systems
- Office furniture

Make sure to create a spreadsheet with:

- Locations
- Make and model
- Age of system (or an estimate)

- Current condition
- Vendors purchased from (invoice number and date, if available) and vendors providing maintenance

In each part of your facility review, make note of areas of concern or potential problems and take corrective measures.

STEP 2: IDENTIFICATION OF EXTERNAL RISKS

There are many different types of external threats that can have a negative effect on your business. To make matters worse, for each threat, there are also many different scenarios that could have different results depending on the timing, location, magnitude, and duration of the event.

Therefore, in this phase, you want to identify and list all potential external threats to your organization, regardless of size or probability. Try to list as many as you can.

At this stage, quantity is more important than quality, so *it cannot be stressed enough that it is important to consider ALL possible risks that could negatively affect your organization.*

Again, not all risks will affect every business in the same area in the same way. Therefore, when conducting your individual risk assessment, you need to consider what threats and disruptions might be unique to you.

With that in mind, here are eight potential external threat or risk areas to consider:

1. **Environmental—**hurricane, tornado, flood, tidal surge, snowstorm, ice storm, extreme temperatures (heat or cold), earthquake, drought, lightning, landslide, mudslide, tsunami, volcano, wildfire, contamination, sinkhole, and meteor
2. **Biological—**flu (H1N1, avian), epidemic, food-borne illness, and infestation
3. **Deliberate Disruption—**terrorism, sabotage, theft, fraud, arson, abduction, kidnap, extortion, bomb threat, demonstrations, civil disturbance, poisoning, workplace violence, and war
4. **Utilities—**loss of electrical power or natural gas supply, loss of water supply, gas and oil shortage, loss of telecommunication service (phone, Internet), and sewer system failure

5. **Equipment—**equipment breakdown, inability to obtain repair parts, major system failures (air conditioning, heating units), and burst pipes
6. **Information Technology—**loss of access to premises, cybercrime, hardware failure, software failure, loss of data or backups, disclosure of confidential data, and loss of skilled personnel
7. **Economic—**new laws or regulations, loss of key personnel, retirement of baby boomers, labor dispute or strike, legal problems, lawsuits, increase in interest or rates, unavailability of capital, changing health-care costs, changes in accounting (revenue recognition, leases), revenue concentrations (major customers, product lines, and geographic region), sole vendors of key supplies, fraud, and theft
8. **Other—**road or bridge construction, public transportation disruption, negative publicity, social media issues, hazardous materials spills, explosions, building collapse, personnel entrapment or rescue, transportation accident (plane, train, or car crash), forced evacuations, changes in technology (3D printers, self-driving cars), and global issues (politics and growth)

STEP 3: DEFINITION OF RISK TOLERANCE

To determine how to address the various types of risks your particular organization faces, you must first define its appetite for risk. In other words, as a whole, is your organization risk tolerant or risk averse?

If you didn't already complete the exercises in step one, take the time now to consider how the various members of your management team approach risk. After you're finished, think about whether your CEO's approach to risk is different from that of the rest of your team.

Another way to evaluate your organization's appetite for risk is to consider its tolerance for failure. Are you encouraged to try new approaches or attempt a new initiative? Are you given time to develop new ideas?

It's also important to define risk in terms of loss. Loss may include:

- Downtime costs
- Impact on customers
- Violation of regulations

Questions to ask include:

- How much money can your organization afford to lose?
- How much server downtime is acceptable?
- How long can you go without access to your data?
- How long would it take for your customers to be affected if your telephone lines or website go down?
- Are there any regulations that specify your maximum downtime?

In some cases, the difference between a minor inconvenience and a major disaster is minutes. Other times, it's hours or days. It also depends on who is affected—an employee, the CEO, one customer, or your entire client base—even varying by department.

The determination of acceptable loss is an important step as it determines the extent of your response plans. Figure 8.3 can help you complete this process.

In this step, also consider how much risk your various stakeholders would be willing to accept. Consider your board of directors, vendors, regulators, customers, and employees. Place the information on Figure 8.4 (or one like it).

Category	**Acceptable Loss (Minimum Downtime or Cost)**	**Unacceptable Loss (Maximum Downtime or Cost)**
Expenses Incurred	$	$
Revenue Lost	$	$
Data/Server Downtime		
Internet Downtime		
Website Downtime		
Telephone Downtime		
# of Employees Affected		
# of Customers Affected		
Departments Affected: ____________________ ____________________		

Figure 8.3 Calculation of Risk Tolerance Range by Category

Stakeholder	**Acceptable Loss (Minimum Downtime or Cost)**	**Unacceptable Loss (Maximum Downtime or Cost)**
CEO		
Board of Directors		
Customers		
Employees		

Figure 8.4 Calculation of Risk Tolerance by Stakeholder

STEP 4: EVALUATION OF THREATS

Because your organization can't possibly address all potential threats to its existence, you need to prioritize them to determine which ones to address first. Each one's extent of risk can be calculated by its potential for damage. In this regard, damage may be assessed in terms of additional cost, impact on employees, lost revenue, and even reputational damage.

An effective evaluation of threats includes:

- An estimation of the likelihood of occurrence
- The potential extent of human, physical, and business impact
- Resources available to address the threats
- The amount of time it will take to return to normal operations

Disaster events may or may not be as risky depending on their characteristics. Figure 8.5 shows a few of the most important ones.

When you consider advance warning, a tornado is riskier than a hurricane because with a tornado, you have seconds to respond, whereas with a hurricane, you usually have several days.

The timing is important as well, as a power outage at night or over the weekend will not have the same effect as one that occurs during working hours. Additionally, a rainstorm that causes two inches of floodwater doesn't have the same physical impact as a fire that destroys the facility and everything in it.

Human impact will also affect risk. For example, bridge construction that affects some of your employees and customers is not as bad as a hurricane that affects your entire region.

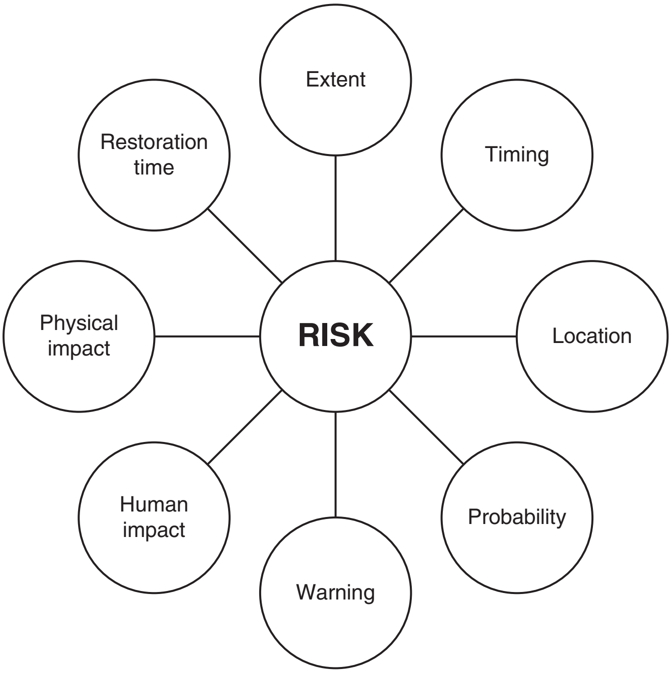


Figure 8.5 Characteristics of Risk

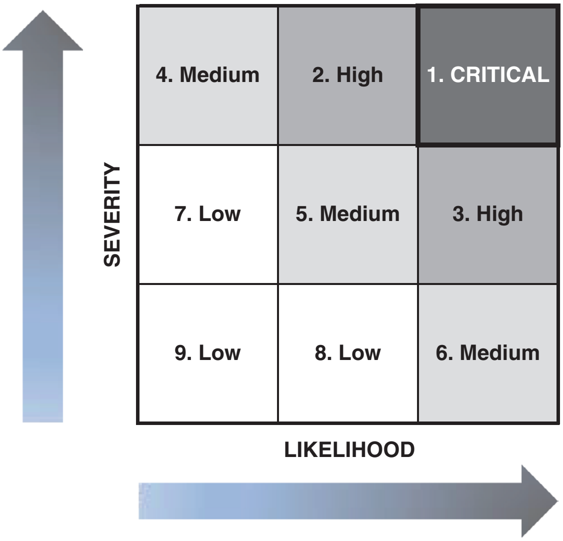
Once you've identified all of the potential risks that could affect your business, it's time to score and rank them based on probability, impact, resources, and restoration time. There are three visual aids you can create to complete a risk analysis. They are a heat map, an impact evaluation, and a risk analysis worksheet.

HEAT MAP

A heat map is a simple visual approach to ranking and rating threats, making it useful for smaller or less complicated organizations. The evaluation of events is based on the likelihood of occurrence (or probability) and the extent of impact (or severity), and the information is posted in the appropriate section. Events ranked high or critical are the threats to address first.

To create a simple heat map, you will need sticky notes and a whiteboard. On the left-hand side of the whiteboard, write "severity" with an arrow pointing up, to indicate that severity increases as you go higher up on the whiteboard. Then write the word "likelihood" along the bottom of the whiteboard with an arrow pointing to the right, indicating that the likelihood increases as you go farther to the right. Next write each of your potential threats on a sticky note. Then stick them to the whiteboard based on your estimate of both the severity and likelihood of the event occurring.

Figure 8.6 is an example of a blank heat map. Each of the squares is numbered based on the urgency with which you should address the potential risk. The risks that end up in "Square 1: Critical" are the ones that are both high in severity and high in likelihood. In other words, they are probably going to happen in the near future and they will have a significant negative impact on your operations. The risks in Square 1 are those that you should address first in your disaster recovery and business continuity plan. The risks that end up in "Square 2: High" are the next set of risks that should be addressed. Although they are lower in likelihood, their impact is significant, and you want to protect against those threats and risks that have the largest, most severe effect on your operations. From there each of the squares is



4. Medium	2. High	1. CRITICAL
7. Low	5. Medium	3. High
9. Low	8. Low	6. Medium

Figure 8.6 Blank Heat Map

numbered based on the order in which they should be addressed in your plan.

IMPACT EVALUATION

The impact evaluation converts the heat map into a dollar assessment. It considers the probability of an event occurring and the potential dollar impact in lost revenue and/or additional costs of the event. To do this type of evaluation, you take the percentage of probability and multiply it by the dollar estimate of cost to create a weighted dollar assessment of each event. The events with the highest weighted dollar impact are the ones you should address first.

Example 1

An organization identifies three potential threats: swine flu, hurricane, and fire. It further estimates that there is a 50 percent probability of an occurrence of the swine flu, with an estimated cost of $40,000. A hurricane is estimated at a 20 percent probability and a $100,000 impact, whereas a fire is estimated at a 5 percent probability and a $300,000 impact. If you consider cost alone, the fire has the greatest effect, and if you consider probability alone, swine flu would be the event to address. But the impact evaluation will consider both sides of the event so, based on the weighting of probability *and* impact, the hurricane is actually the biggest threat and should be addressed first.

Event	**Probability (%)**	**Impact ($)**	**Total (% × $)**
Swine Flu	50	40,000	20,000
Hurricane	20	120,000	24,000
Fire	5	300,000	15,000

RISK ANALYSIS WORKSHEET

The risk analysis worksheet is a more detailed and thorough approach to evaluating threats based on probability, impact, available resources, and restoration time. A copy of one is included in Appendix B.

For each column, you evaluate the field using a scale of 1 to 5, where 1 is the least likely or least amount of impact and 5 is the greatest likelihood or greatest amount of impact. This will tell you which threats should be addressed first. (Note: The rankings are subjective and you can allow for some interpretation, but whether you rank an event as a 3 or a 4 is not likely to change the outcome of the analysis.)

STEP 5: RISK RESPONSE

After completing your risk analysis, review your top five threats and look for consistencies and similarities between them. For example, you may have listed a hurricane and a power outage. While the hurricane has greater human and property impact, the greatest impact to you may be the loss of power.

Also, look for similarities regarding resources. If you don't have the necessary resources to respond, maybe you can correct that situation. Can you provide more training? Purchase equipment or supplies?

Another part of risk analysis is determining how your organization wants to address each threat. For each identified threat, determine whether you are willing to accept the threat, avoid it entirely, or take steps to mitigate the impact. Mitigation may involve obtaining insurance, taking steps to prevent or reduce the impact, or both.

Each organization has to evaluate the potential impact of its individual threats in comparison to its tolerance for risk and the potential for long-term business impact. For each company, these will be different.

STEP 6: MONITORING

Once the analysis is completed, it should be updated, at a minimum, once a year. Monitor your organization, customers, vendors, and external environment for changes that may create a new risk or change the ranking of an existing threat. New threats may appear or you may develop new capabilities to address existing threats.

THREE RISK ASSESSMENT METHODS TO CONSIDER

Expanding on the risk assessment process further, it's important to realize that there are a variety of tools available to help you better identify the various internal and external threats to your organization. These include employee surveys, PESTLE analysis, and SWOT analysis.

EMPLOYEE SURVEYS

A simple method for collecting a list of potential threats to your company is to ask your employees. They are the ones most familiar with the day-to-day operations of your organization, which also means that they know where its weaknesses are.

To perform an employee survey, simply send out an inner office questionnaire asking employees for their opinions of risk. Questions to ask include:

- What risks could interrupt our business?
- How could our business fail?
- What must we do well in order to succeed?
- On what information do we most rely?
- What assets do we need to protect?
- How could someone or something disrupt our business?
- Which employees are most crucial to our success?
- Which employees have the most knowledge of our operations?
- How could someone steal from the organization?

Answers to these types of questions can give you great insight as to risks that you may not even know to exist.

PESTLE ANALYSIS

PESTLE stands for political, economic, social, technological, legal, and environmental, and this type of analysis is an effective tool for brainstorming the greater external environment in which your organization is operating. Use it and you have an easier time identifying the underlying risks associated with these six factors.

1. **Political.** Political factors include potential changes in regime, tax policies, fiscal policy, trade tariffs, wars, seizures of property

or technology, regulatory bodies, current and future legislation, and trading policies that may either affect the business environment in general or your industry in particular. Essentially, you want to consider the extent to which a government may influence the economy or your industry.

2. **Economic.** Economic factors include inflation rate, interest rates, foreign exchange rates, economic growth patterns, employment rates, distribution trends, and market and trade cycles. Think about the current and future of the economy's performance and how it may directly affect your organization in the long term.
3. **Social.** This factor requires that you consider the social aspects of the market and gauge the potential impact of cultural trends, demographics, lifestyle trends, consumer attitudes, fashion and role models, advertising and publicity, trending topics on social media, and media perspectives on your business.
4. **Technological.** Technological factors include emerging technologies, rate of change, licensing, patents, communications, dependent technologies, and obsolescing technologies. Consider the impact of technological innovations and how they might affect your operations, the industry, or the market.
5. **Legal.** Legal factors encompass consumer laws, safety standards, labor laws, enforcement and penalties, and the litigation climate. How will the overall legal environment in your industry, your state, and your country impact your business?
6. **Environmental.** Environmental factors to consider include the impact of your operations on the environment, use of diminishing resources, climate and weather, your geographical location, and consumer and political attitudes toward environmental issues. What's the potential for current or new environmental regulation that could ultimately affect your organization and the way that you do business?

There are many variations of the PESTLE analysis (PEST, PESTLI, PESTLIED, STEEPLE, SLEPT, and LONGPESTLE). However, each one has the same basic overall goal, which is to answer these six questions:

1. What is the political situation in the countries we operate in?
2. What are the current local and global economic trends?
3. What are the major social and cultural factors in our market?
4. What is the impact of technology on our organization?
5. What is the current status of legislation and regulations that affect our industry?
6. What are our environmental concerns?

SWOT ANALYSIS

SWOT analysis is yet another brainstorming tool that helps you better identify the positive and negative effects of both internal and external factors. SWOT stands for: strengths, weaknesses, opportunities, and threats.

> It's important to note that *strengths* and *weaknesses* are *internal*. Opportunities and threats are *external.*

Strengths. Strengths are internal to your organization and include such factors as expertise, people, finances, innovation, process, and market share.

Consider what your organization does better than anyone else. What sets you apart from your competition?

- Competitive advantage
- Unique selling proposition
- Experience and knowledge
- Proprietary information (technology or process)
- Personnel
- Innovation
- Price
- Quality
- Value
- Systems
- Management and leadership

- Culture
- Philosophy
- Ethics
- Reputation
- Market share
- Cash flow
- Finances

Weaknesses. Weaknesses are also internal to your organization and relate to your products, market, production, process, or people. What weaknesses can be improved?

Factors to consider include:

- Disadvantages of proposition
- Gaps in capabilities
- Financial weaknesses
- Lack of market share
- Supply chain vulnerability (like if you have one sole supplier)
- Reliability of data
- Vulnerability of computer systems
- Continuity of management
- Workplace morale
- Safety
- Reliance on significant customers
- Limited geographic distribution

Opportunities. Opportunities are different than your strengths and weaknesses in that they are external to your organization.

This means that you need to look outside of your operations to:

- Customers
- Vendors
- Market
- Region
- Technology

Take into account what is going on in the world that might provide an opportunity *to increase market share and revenue* . . . or *increase efficiency and decrease costs.*

This includes taking a closer look at:

- Your competitor's weaknesses
- Industry trends
- Demographic trends
- New markets
- Changes in technology
- Corporate partnerships
- Product development
- Global influences

Threats. Threats are also external to your organization and, as with opportunities, brainstorming threats involves looking outside of your operations to customers, vendors, market, region, and technology.

What's going on in the world that might create decreased revenue and decreased market share? What's going on in the world that might increase costs or reduce efficiency?

Factors to consider include:

- Increased competition
- Competitor strengths
- Political effects
- Legislation and regulatory effects
- Softening market
- Environmental effects
- Weather
- Economic timing (local, national, global)

Performing these three types of risk assessment can help you better understand the vulnerabilities in your business so you can better respond to disasters. Depending on how much risk you assess each particular event, it may go into one of three categories:

1. **Planning.** Planning is the best approach for low-probability, high-impact events. While these events are not likely, you should

still have a response plan in place to deal with them because they would have a significant negative impact if they did happen.

2. **Acceptance.** Disasters in this category aren't likely to happen and wouldn't have a large impact even they did. Thus, accepting the risk is the best approach for low-probability, low-impact events like these because it's most cost-effective to assume the risk on the very slight chance they might occur.
3. **Containment.** Containment is the best approach for high-probability, low-impact events because (if at all possible) it's good to try to minimize the likelihood of occurrence while still preparing to minimize the likely damage.

ASSIGN A CHIEF RISK OFFICER

Every project needs a leader, someone assigned the responsibility for getting the project done and keeping it up-to-date, and risk management is no different. That's why you need to designate a chief risk officer, or CRO.

In some organizations, the CRO is a separate position. However, small companies may not be able to hire a separate CRO. If this is you, that's okay. Just assign the related responsibilities to someone in the organization.

The CRO is a leader, facilitator, and coordinator who identifies and monitors both threats to the organization and related opportunities. He or she will take a big-picture approach to bringing negative and positive issues to the attention of management.

The first responsibility of the CRO is to monitor the organization's appetite for risk and acceptable risk limits.

In addition, the CRO is responsible for developing a process to: identify, analyze, monitor, and report on risks and opportunities.

He or she will also be tasked with:

- Coordinating safety (and risk) training
- Developing risk action plans
- Leading the business continuity planning team
- Leading the emergency response team

The CRO should have a thorough knowledge of the industry and the company's internal business processes. He or she should be analytic, proactive, and decisive, and adapt well to (and be capable of) initiating change in the organization. This person needs good written and oral communication skills, solid presentation skills, and be good at project management.

Questions to Ask Yourself

1. What potential safety risks do our employees, customers, vendors, and other stakeholders face?
2. What are some of our biggest physical vulnerabilities?
3. What types of external risks does our company face?
4. How will we respond to each one? Acceptance? Avoidance? Mitigation?
5. What is our risk tolerance?
6. How can we use employee surveys, a PESTLE analysis, or a SWOT analysis to identify our biggest risks?

CHAPTER 9

Step 6: Determine Recovery Strategies

Disaster response occurs in three stages:

1. Prevention
2. Incident response
3. Business continuation

To help better understand what each one involves, think of them the same way you would a medical response to a heart attack.

There is the prevention phase, which is when the doctor advises you to eat right and get exercise. The incident response phase is when a heart attack occurs and someone calls 911. The EMTs arrive and do their best to prevent further damage, transporting you to the hospital.

The business continuation phase corresponds to when you are released from inpatient care and begin outpatient therapy. The crisis is over, but there are still steps to take before you're fully functioning and have returned to normal.

Let's dive a little deeper into each one now and discuss how it relates to a business disaster response.

PREVENTION

For every type of disaster, an organization can respond multiple ways. That being said, the first thing it should *always* do is ask: "How can we prevent the disaster from occurring?"

Just as a doctor will tell you that the best way to treat a disease is to prevent it, the most cost-effective way to respond to a disaster is to keep it from happening in the first place. Thus, the most effective disaster response process should begin long before disaster even strikes.

Inevitably, someone says, "But I can't prevent a hurricane!" Although that is true, you *can* prevent the hurricane from turning your business into a disaster area by having a well-thought-out response plan that addresses the issues this type of event would create for your business.

There are many steps an organization can take to prevent or mitigate potential damage from a disaster. However, it's important to consider both prevention and mitigation separately as prevention involves taking steps to prevent damage from occurring, whereas mitigation involves taking steps to reduce the impact of damage that has already happened.

When creating your prevention plan, think about the actions you need to take (and in what order they should be taken) to prevent:

- Death or injury to employees (or visitors)
- Destruction or damage to facilities, equipment, vehicles, records, and information

For best results, involve all of your employees in this process! People working at different levels in the organization have differing perspectives and will provide a variety of ideas for preventing damage.

Fundamental preventative steps include:

- Ensuring that your address is clearly marked
- Installing:
  - Fire sprinkler systems
  - Storm shutters
  - Emergency lighting system
  - Shatterproof glass windows
- Moving all heavy or breakable objects to lower shelves
- Covering and moving computers up and off the floor, placing them (and their corresponding workstations) away from windows
- Securing any exterior signs and equipment on rooftops. Make sure your building entrances and emergency exits are clearly marked and easily accessible. Trim trees and shrubs so that they won't puncture windows.
- Purchasing additional fuel for generators or heating systems. Double-check that all pathways and parking areas are well lit.

In advance of an emergency, you should also stock up on emergency response supplies. This may include the purchase of:

- Safety equipment (goggles, respirators, safety suits, gloves)
- Potable water

- Nonperishable food
- Can openers and eating utensils
- Battery-powered radios (Broadcast, S.W., and VHF)
- Extra batteries
- Flashlights
- First aid kits
- Sanitation supplies (paper towels, moist towelettes, disinfectants)
- Basic tools (pocketknife, wrench, pliers, hammer, duct tape)
- Garbage bags
- Blankets and pillows
- Personal hygiene (toothbrushes, toothpaste, soap)
- Extra clothing
- A whistle, to signal for help
- Cell phone chargers
- Solar chargers
- Fire extinguishers
- Matches
- Local maps
- Company letterhead and checks

INCIDENT RESPONSE

On August 23, 2011, a 5.8-magnitude earthquake struck Central Virginia. Seventy miles away, in Maryland, I was working in an eight-story building.

None of the employees had ever experienced an earthquake, so no one had any idea what was happening or what to do. Apparently, no one else in the building had any idea either as there was a massive stampede of people trying to leave the building, most via the stairs, but some by taking the elevator.

People congregated in the parking lot and rumors flew as to what happened. Cell phones didn't work for more than an hour, there was no one in charge, and confusion reigned. No one knew if the building was safe to enter, yet most of us had left the building without car keys, purses, or wallets so we were stuck.

Proper incident response planning helps avoid these types of situations because the plan specifically states the steps you'll take at the inception of the disaster. It also says how you intend to minimize injury, property damage, and overall impact.

Emergency care and first aid are the top priorities. Provide medical care if necessary. It's always a good idea to make Red Cross first aid training available for employees. Medical care includes employees, visitors, vendors, and anyone else who was on your grounds when the disaster occurred.

Once everyone has been tended to, conduct an analysis of the situation. Make an initial assessment of the problem, the extent of the damage (*Appendix C has a sample form you can use*), the safety of the facility for reopening or reentry, and the resource requirements for managing the response.

Assign this particular responsibility to someone with a cool demeanor who has skills, knowledge, and expertise in disaster assessment. When something major happens, employees will be shaken, both expecting and seeing the worst. Having an individual who can calmly and honestly assess the situation will help reduce the chaos and hysteria.

A lockdown may be necessary (such as a perpetrator inside or outside of your facility who appears intent on committing acts of violence). The primary goals of a lockdown are:

- To protect those who are trapped or unable to evacuate the building
- To prevent additional unsuspecting people from being exposed to the situation.

A lockdown situation requires an immediate and far-reaching warning message to employees and visitors alike, but it's also important to consider whether it's safer to issue a lockdown alert silently. Employee training should cover both types of lockdown procedures, including other valuable responses, such as hiding under desks, locking and barricading doors, staying away from doors and windows, and staying in place until notified that it's safe to evacuate the building.

In the case of a disaster like a tornado or earthquake, you may have just minutes or even seconds to gather your belongings and get out of the facility. Would your employees know what to take with them? Would they know where to go? Because there's no time to think through a response on the spot, planning for an evacuation is crucial.

The first step in preparing an effective evacuation plan is to identify where you'd like your employees to congregate in the event they are forced to leave the building. Once you've identified the location or locations, map out the exit routes from your facility. Create a subsequent process to account for employees to ensure they're all safe and sound.

Train your staff to respond *immediately* to an evacuation alarm. If there's time and the response is efficient, they may be able to grab personal items, such as a cell phone, laptop, wallet or purse, and car/house keys. Building access cards are also important for when it's safe to reenter.

If you can, take first aid supplies with you. It's a good idea to designate a manager to take first aid supplies in the event of an emergency. If there's enough time, you may also choose to grab backup tapes, flash drives, or other basic office supplies. The key is to take what you can without sacrificing your own personal safety to do it.

A third incident response is to shelter in place. A shelter-in-place strategy is used when you can't leave the building. This may be the result of a hurricane, tornado, or hazardous material spill.

Depending on the type of emergency, the plan should include procedures to warn everyone to move away from windows and into the core of the building or to higher floors. It should also have a way of advising anyone working outside that they need to enter the building immediately.

Create procedures for everyone, once in place, to stay sheltered until it is safe to evacuate the building. Consider the needs for space, food, water, sanitation, and sleeping facilities during this time.

When dealing with a disaster, you need a clear chain of authority and accountability, with one person in charge. This person will:

- Oversee the emergency response
- Conduct a situational analysis

- Implement your response plan
- Provide crisis communications

BUSINESS CONTINUATION

The third and final portion of your disaster response plan is business continuation. This is the part of your plan where you address the steps you need to take to start operating your business again *after* the initial response to the disaster.

When preparing this portion of the plan, some of the things you want to consider include:

- Where can we conduct business, if not at our own facility?
- How will we get necessary supplies?
- How will we deliver products to our customers?
- How will we process payroll?
- How will we pay for the things we need?
- How will we maintain our accounting records?
- Who will process the insurance claims?
- How will we handle personnel needs?
- How will we restore our IT systems?
- What business functions need to be restored? In what order?

Although this may seem a bit overwhelming, remember that as long as you have resources in place in six key areas you'll be in good shape:

1. Personnel
2. Workspace
3. Equipment
4. Forms and documents
5. Special supplies
6. Critical information

With regard to personnel, you want to first identify the critical functions and then identify the critical personnel. These are the employees who need to get back to work sooner because they're responsible for these tasks.

When it comes to workspace, there are a few questions you'll need to answer. For instance, what type of workspace will you need in the event of a disaster? Can you operate in just a portion of your building? Do you have an alternate location available if your facility is destroyed?

For equipment, what equipment will be necessary to operate your business? Do you have specialized equipment? What office equipment would you need (phones, copiers, computers, etc.)? Can your equipment be prepared, rented, or replaced?

Additionally, *what forms, documents, and information cannot* be replaced (like contracts or patents)? What unique supplies do you need in production? Do you have alternate vendors?

With regard to your critical information, what information and data do you store, and where?

If you live near the coast (or in a flood-prone area) do you store documents well above the 100-year flood zone? Maybe you want to pay someone extra so that in the event of a disaster your documents get priority evacuation to safe storage, so they won't be destroyed? How will you recover or access the data after a disaster? What critical information do you need to access immediately, such as building plans, formulas and trade secrets, or personnel files?

COMMUNICATIONS DURING A DISASTER

The need to communicate during an emergency occurs immediately as the ability to instantly respond may mean the difference between life and death for the employees *and* the organization. Plus, questions typically start arising long before the disaster is even over.

Different people will want different information, but they will all want it right now! Employees will need to know what to do. Their families will be concerned and want information. State and local officials, as well as regulators, may need to be notified. Surrounding businesses and neighbors may also need to be informed.

The stakeholders will also want information immediately, often before you've had a chance to activate communication plans. Thus, an effective disaster response is dependent on your organization's ability to respond promptly and effectively during a disaster (as well as in the subsequent hours and days) and to communicate that response. Though this may feel overwhelming, the payoff is there.

For instance, I recently traveled to Columbus, Ohio, and stayed in a hotel. The local news came on announcing tornado warnings for various parts of the area. Shortly thereafter, I heard sirens outside, so I immediately called the front desk to ask what was happening and what I should do. They had obviously been trained in crisis communications because they calmly and clearly explained the situation and what steps would be taken. As a customer, I was impressed by the response and my mind was instantly put at ease.

Although that situation worked out well, one of the primary difficulties of communicating during a disaster is that many of your normal channels for communication become unavailable. Phone lines may be down, cell towers may be down, or cell phone systems may be overloaded. Power outages or cable system failures may prevent access to the Internet. That's why your communications plan should provide for alternate methods of communication. It makes sense for the company to buy or rent satellite phones for management to keep critical communications open when all else is chaos!

You should also include procedures for notifying personnel of an impending disaster. The procedures should also include the steps to take for any subsequent communications to employees, customers, and vendors after the disaster occurs. This includes communicating with company directors, investors, government and regulatory officials, families of employees, the media, other impacted individuals or businesses, and affected external organizations.

To help prepare this type of plan, you must first know what types of communication systems you currently use. *A sample form for capturing this type of information can be found in Appendix D.*

INFORMATION TO INCLUDE

A complete communications plan includes an emergency contact list with contact information for employees, vendors, customers, and any other emergency contacts you deem fit. Because this information typically changes often, it's important that it is updated regularly. At a minimum, it should include each person's:

- Name
- Home and cell phone number
- Personal e-mail address
- Alternate contact information (usually a family member or friend)

For vendors and suppliers, you'll also want to include the business name, website address, individual contacts' names, the positions of those contacts, and contact information for each of these individuals.

PREPARATION AND COORDINATION

Because things tend to get chaotic in times of disaster, it's a good idea to prepare scripted messages in template form. Because they're created in advance, they should be developed and approved by the management team. Once completed, make sure they're accessible to the appropriate people from any remote location.

It's also a good idea to assign one person the responsibility of coordinating disaster communications. This way, the messages are more likely to be consistent, accurate, and on point. It will also ensure that necessary calls will be made and not slip through the cracks.

For example, if someone needs emergency medical services, who will call 911? In many cases, employees become so focused on responding to the issue at hand that they assume that somebody else will make the call. It's only when emergency personnel don't arrive that they realize that no one initiated the contact.

Another consideration is whether your notifications need to be bilingual or multilingual. Obviously, this depends on the makeup of your workforce and external stakeholders, but it's definitely something to think about and consider addressing if your group is more diverse.

NOTIFICATION SYSTEMS

Creating an alert notification system with multiple means of communicating with your employees, vendors, customers, and other stakeholders can be beneficial as you never know what types of issues certain disasters will bring.

Your notification system might include verbal announcements, automated phone calls, texts, e-mails, a phone system message, internal website notifications, and social media. Most important, whatever avenues you choose, test them on a regular basis to verify that they're going to be effective.

Be aware that during widespread disasters, cell phone systems often become overloaded and calls cannot be completed. *Text messages, however, because of their brevity, are likely to go through, so consider making this form of communication part of your overall plan.*

EMPLOYEE COMMUNICATIONS

Your employees must understand your emergency communication system or it's never going to work. This means integrating crisis communication plans into your new hire's onboarding process as well as conducting additional training throughout the year.

Even though employees are an organization's most valuable asset, if a disaster occurs, the human side is often overlooked. Don't do that to your team. Instead, spend the time and effort necessary to help them deal with the shock and stress of a disaster.

If it's a major disaster, they may be suffering as much as your organization. Maybe they've lost their home or lost a loved one. Most people aren't prepared for the psychological effects of these types of events, so do your best to help them through it.

Expect that in the first 24 hours after a disaster, employees will likely be numb, in denial, physically sick, anxious, or withdrawn as they're trying to cope with the disaster's impact on their personal lives and their families, as well as their work issues. In the week following, they may begin to feel isolated, anxious about the future, or angry at the situation. They might withdraw from contact or become more demanding.

Depending on the individual impact, the person's coping abilities, and support systems, there may be longer-term effects that will need to be addressed. Additionally, know that after a disaster, employees may be more prone to exhaustion and burnout.

To assist employees after a disaster:

- Encourage communication about the disaster and its effects.
- Consider allowing for flexible schedules, a leave of absence, or reassignment to a new position.

- Encourage supervisors to watch for changes in behavior.
- Establish a wellness program.
- Set up a formal employee assistance program.
- Provide lunchtime learning sessions.

SPECIFIC CONSIDERATIONS

Your communications plan should also include ways to address the various needs of your stakeholders and other specific groups who will be interested in different types of information.

For instance, *management* will likely want to know:

- What happened and when
- Whether anyone was injured or killed
- What the extent of property damage is
- How long it will take to resume normal operations
- What the potential is for liability

Employees (on the other hand) tend to be most concerned about:

- What happened
- When it will be safe to go back to work
- Whether they'll get paid during the shutdown

Often, customers become aware of a problem when phone calls and e-mails aren't answered or electronic orders aren't processed. Therefore, if your phone or Internet system goes down, your plan should include a way to redirect these messages and respond to them, indicating that your business is experiencing a temporary problem.

Also, be prepared to discuss *customers'* questions regarding:

- Status of their order
- Potential delays
- Cancellations
- Possible compensation

The more you decide this information beforehand, the less likely it is you'll be faced with a situation where you're unsure what to do.

Vendors will also want to be able to find out about orders previously placed.

- Are they still able to be delivered?
- Are the orders to be delayed?
- Are the orders to be canceled?
- Do they need to ship to an alternate location?

Note: Governmental or regulatory requirements regarding communications depend on the type of incident and its severity. This makes it extremely important to be very clear about when you are mandated to notify a regulator as the penalties from a delay or failure to notify can result in possible jail time.

Be ready to report details about:

- When the incident happened
- The incident itself
- The impact caused (such as injury, death, property damage, contamination, and consumer safety issues)

Again, depending on the type and extent of the disaster, nearby businesses and residents may want to know if it's safe to go outside or safe to return. They'll likely also want information about how they'll be compensated for any loss they incurred and what will be done to prevent the disaster from happening again.

In the event of an emergency, communicate with the public as soon as you can. If you don't, rumors will spread, and some people will just assume that you've already gone out of business.

To avoid these types of situations, appoint one person as spokesperson to respond to inquiries and provide information in a clear and unemotional manner. This can reduce stress and the likelihood of lawsuits, while maintaining your company's reputation at the same time. (*Appendix E is an Emergency Communications Summary, which contains all of the information this person would likely need.*)

This person should also be the one who speaks to the news media because they'll want to know *everything*... and then some. They'll ask what happened, who was injured, what the extent of loss was, who and/or what caused the problem, what the long-term effect is, how you will prevent it from happening again, and so on. They'll ask it all, so this person needs to be prepared!

If there is extensive damage to other people's property caused by your company, it makes sense to hire a PR firm with in-house legal counsel to make sure that public statements to the press do not cause undo complications.

Although it may not always be pleasant to cooperate with the media, trying to avoid them will only make matters worse. Simply prepare a written statement in advance that expresses your concern for the safety of everybody involved and regret over any injuries or damage suffered during the disaster. Remember that *people come first*, so focus on your attention to their health and well-being before covering anything in relation to property damage and lost revenue.

Additionally, when they ask their thousands of questions, always tell the truth and don't speculate or spin. If you don't know the answer, say so. If possible, avoid estimates of monetary damage or the time it will take to return to normal, just in case you're wrong. This alone can save you a ton of grief.

Questions to Ask Yourself

1. What types of prevention strategies can our company put in place to help prevent a disaster or minimize its damage?
2. What type of incident response plan makes the most sense for our business?
3. Who should be responsible for our communications?
4. Which individuals and businesses do we need contact information for?
5. Where should we keep our prearranged message responses so that the appropriate people have access them?

CHAPTER 10

Steps 7–10: Create, Communicate, Test, and Regularly Update Your Written Plan

Because all of the remaining steps occur in quick succession, one right after the other, they're grouped together in this chapter. However, if you noticed the section title, the creation of the written plan will come first.

A COMPLETE BUSINESS CONTINUITY PLAN

When all is said and done, your written business continuity plan (BCP) should answer all of the questions that could possibly come up during a disaster. Some of the most common are:

- Where else can we work from? What are potential alternative physical locations?
- How will we get our work done? What alternate computer systems can we use and what software applications and data are critical?
- Which of our employees needs to be back at work first?
- What equipment do we need to keep working? If it's damaged, can we rent, repair, or replace it?
- Who will provide our materials if a vendor is impacted? Do we have alternate suppliers?
- How will we pay our bills?
- How will we keep track of transactions?
- How will we process payroll and pay our staff?
- How will we handle the insurance claim?
- How will we interact with the community and our stakeholders?

Admittedly, coming up with how you're going to present all of this information clearly and concisely in one neatly written plan can feel a little overwhelming. That's why it helps to break it down into smaller pieces, each of which feels a whole lot more manageable.

With that thought in mind, the six basic components of a complete BCP are:

1. Executive summary
2. Introduction
3. Business continuity strategy

4. Disaster response team
5. Disaster response
6. Supporting documents

EXECUTIVE SUMMARY

The executive summary is an overview of the contents of the plan and should include its purpose, the authorities and responsibilities of key personnel, the definition of a disaster, a list of the types of expected emergencies that are covered, and where operations will be managed.

INTRODUCTION

The next section is the introduction, and this is where you'll address how to use the plan, as well as its objectives, scope, and assumptions. It's basically an overview of the process, which is why it should contain information about the plan maintenance, testing procedures, training procedures, and plan distribution.

BUSINESS CONTINUITY STRATEGY

The business continuity section of the plan describes the overall approach to disaster management. It shares the elements related to all emergency procedures the organization will follow to protect personnel and property and to mitigate the impact of the disaster.

This portion of the plan is where you talk about:

- The location of your emergency operations center
- Communication protocols
- Safety responsibilities
- Relocation strategy
- The recovery plan phases (including occurrence, activation, and alternate site operations)
- Property protection, recovery, and restoration
- Critical records
- Administration and logistics
- Access to computer systems
- Community outreach

DISASTER RESPONSE TEAM

The disaster response team section of the BCP identifies the team members and their responsibilities. Assignments typically include:

- Business continuity coordination
- Communications
- Human resources
- Emergency response
- IT recovery (which is covered more in-depth in a later chapter). It also contains their contact information and levels of authority.

DISASTER RESPONSE

The disaster response section spells out the procedures your organization will execute when responding to an emergency. Because it can be difficult to read a lengthy document during the chaos of the disaster, *whenever possible, these procedures should be formatted as a checklist or a map*. The goal is to make it as easy as possible for people to follow when they're under massive stress.

Disaster response procedures should include:

- Procedures for accounting for all employees and visitors after an evacuation
- How to assess the situation
- How and when to activate the disaster response
- How to report an emergency
- Who to report the emergency to
- Procedures for communicating with personnel
- Procedures for protecting employees, visitors, customers, records, critical equipment, and the facility
- Rescue and medical response protocol
- How and when to order an evacuation
- Specific procedures for responding to particular events, such as an earthquake or tornado
- Instructions for managing response activities
- Coordination efforts with outside organizations

- Procedures for shutting down operations
- Procedures for returning operations to normal
- Procedures for determining when a disaster is "over"

SUPPORTING DOCUMENTS

During and after a disaster, the records you would normally have easy access to often become a lot more difficult to get your hands on. Thus, keeping secondary copies with your disaster recovery plan can make life much, much easier.

Supporting documents may include:

- Emergency call lists
- A list of your physical locations, including street addresses
- Building plans and blueprints, including locations of exits and stairways
- Emergency escape routes
- Utility information, including types and locations of main valves or main shut-offs
- Locations of fire exits and fire suppression systems
- A list of stored hazardous materials
- Property listings
- Resource lists, including:
  - Insurance summaries
  - Financial and banking information
  - Mutual aid agreements
  - Significant vendors and customers
  - Disaster response supplies

For your convenience, a *Business Continuity Plan Outline can be found in Appendix F.* This can serve as a basic guide to ensure that you've hit all of these main components, making your plan complete.

A BASIC BUSINESS CONTINUITY PLAN

Admittedly, a BCP can be an expensive and lengthy document. And though we've just covered all of the elements of a full-blown plan, a smaller, basic plan is always better than no plan at all.

So, if you're a smaller business or the idea of creating a complete BCP scares you to the point that you'll never do it, creating a basic BCP is the next best thing.

Basic BCPs have six key elements that can be summarized simply in a short document. These elements are:

1. A list of key contacts and their contact information (during and after normal business hours)
2. A checklist of immediate response actions required in a disaster
3. The responsibilities of various staff, especially for the emergency response team
4. Information establishing who has authority over what types of decisions
5. A communication plan
6. Supporting documents (including insurance information, banking information, and vendor and customer lists)

If your company is big enough, divide these pieces and assign specific sections to different people. Additionally, it may be appropriate to use distinct formats (written paragraphs, lists, or checklists) for different sections.

To ensure the plan is completed in a timely manner, set a timeline for completion of each section. It also helps to assign one person to be the "document manager."

This person oversees the writing process and the timeliness of creating the plan. He or she also has the responsibility of ensuring that each section is thorough and accurate, that the plan is safely stored and accessible to those who need it, and that it is updated on a regular basis.

AFTER THE PLAN IS WRITTEN

Once the first draft is written, allow other members of the team to review it for understandability and completeness. Take their input and create a second draft. Then, when that's completed, the next step is to perform a "tabletop" exercise.

A tabletop exercise is when the planning team sits at a table and walks through the written plan to see if any parts are unclear or missing. If you do that and it appears complete, follow up with a live drill to see if anything changes when you attempt to fully implement your procedures.

For instance, two critical components that often show up in a live drill are how to address the needs of disabled persons and non-English-speaking personnel. These types of issues may need to be discussed and added into your plan.

Once you're confident that your written BCP will be effective, print it, store it, and distribute it to all employees as they're the ones who need to understand and know how to use it. Distribution also helps integrate your emergency planning process into the company culture.

Every employee requires some form of training in disaster response, and this training may take various forms. It can be conducted through memos, discussion sessions, workshops, a tabletop exercise, or practice drills. It is essential that a member of the C-suite becomes the organization's safety officer. In an emergency it is critical that one person (and an assistant) understands the big picture and can coordinate with department heads. Whatever emergency methods you use, they need to be practiced on a regular basis.

Development of an employee training plan should be done by your safety officer and members of your business continuity team. When creating this plan, consider the different training needs of employees, visitors, managers, emergency response team, and others (such as vendors). Veterans (especially Navy and Coast Guard) often already have extensive experience with emergency planning and procedures.

If possible, plan your training one year out and include who will be trained, who will conduct the training, the forms of training, when and where the training will occur, and how the training session will be evaluated and documented. *Appendix G contains a sample scheduling chart to help you keep track of your training and testing exercises.*

Consider also training needs for certain situations, such as when you hire new employees, purchase new equipment, start using new materials, change the layout or design of your facility, or revise your emergency procedures. At a minimum, all employees need to know:

- The purpose of the plan
- The types of emergencies that might occur

- Their roles and responsibilities during a disaster
- The appropriate response in specific situations
- The roles and responsibilities of key personnel and emergency response team
- Warning and communication procedures
- Evacuation, sheltering, and accountability procedures
- The location and use of common emergency equipment
- The location of first aid supplies
- Emergency shutdown procedures

PRACTICE YOUR PLAN

As the old adage goes, practice makes perfect. So, just as you practiced fire drills in elementary school, it's important to have your employees practice the disaster response plan by participating in tabletop exercises, walk-through drills, evacuation drills, or full-scale exercises.

We've already talked about tabletop exercises briefly, but, as a reminder, they don't require a special location as they can be conducted in a conference room setting. In this exercise, employees simply discuss how they'd react to a disaster, including the specific the steps they'd take and in what order. This exercise is an efficient way to identify areas of overlap, confusion, or missing parts to the plan.

A walk-through drill consists of the emergency response team actually performing their functions. This type of exercise *is* more thorough and time-consuming, but it also provides invaluable training for the people who are directly responsible for a quick response.

Evacuation drills involve employees actually evacuating the building by taking designated routes and meeting in the designated areas, so they can all be accounted for. As they would during an actual evacuation, they should use the stairs as opposed to elevators. Also ask them to take note of potential hazards during an actual emergency, such as cluttered hallways or doors that are difficult to open.

In a full-scale exercise, a real-life emergency is simulated as close to reality as possible. This typically involves coordinating with local emergency response personnel (police, fire, EMS) and community response organizations (Red Cross) and working together to practice the best possible response.

After completing any of these types of exercises, consider involving your employees, community responders, and anyone else who took part in the process in an informal evaluation. Share the lessons each of you learned and use them to improve your procedures, update your manuals, and provide better training.

Questions to Ask Yourself

1. Based on the size of our business, should we have a complete written business continuity plan, or will a basic plan suffice?
2. Who will compile each section?
3. What supporting documents do we need?
4. What types of trainings can our organization realistically engage in?
5. What other agencies should be involved?

CHAPTER 11

Insurance Coverage

Many businesses have a love-hate relationship with insurance. We love the security it provides but hate the cost. We know we have to have it, yet hope we never have to use it. It's the proverbial Catch-22 . . . we can't live with the risk, but we also can't live with insurance costs.

Then there's trying to figure out all of the technical (and typically confusing) insurance-related terminology, exclusions, and exceptions to the exclusions. Even after reading every page of an insurance policy, most of us aren't exactly certain of the coverage we're getting. But we *are* certain of the cost.

That being said, one of biggest issues organizations deal with after a disaster is cash flow, especially when recovery includes cleaning up damaged areas, making repairs, and replacing equipment. All of these things cost money. Worse yet, they cost money at the same time that your revenue stream is diminished, if not completely stopped.

Then there are the fixed costs that still need to be paid on a regular basis. For instance, your landlord doesn't want to wait to receive rent, your bank still wants its loan payment, and employees still want their fairly earned dues. So what are you to do?

PREDISASTER FINANCIAL PLANNING

The best thing you can do for your company is preplan for the cash flow crunch that typically comes with a disaster. Depending on your circumstances, this may involve arranging for a line of credit, self-insuring, or obtaining commercial insurance coverage.

ADVANCED LINES OF CREDIT

Many businesses mistakenly assume that loans or lines of credit will be available through the Small Business Administration, FEMA, or their local Emergency Management Office during a disaster. Yet, the sad truth is that not every business impacted will qualify.

Additionally, even if you are one of the lucky ones to meet the minimum requirements, the amounts available may not be sufficient to cover your cash flow needs. Then there's the issue that the loans may not be ready right when you need the money because of the length of time it takes to process and approve your application.

It's also not uncommon for the facilities and equipment used as collateral to be damaged or destroyed in a disaster situation. If this happens to you, you may not comply with the covenants for those loans. The end result is extreme difficulty when it comes to obtaining commercial financing in an emergency situation.

Remember also that banks don't like to lend money when you really need it! So, if you plan to use a line of credit to protect your cash flow, make sure it's in place long before a disaster appears on the horizon.

SELF-INSURANCE

Although not technically "insurance" because this term generally refers to a contract where an insurer agrees to pay the insured for a covered loss (in other words, an outside party bears the financial responsibility for *your* loss in the event that one occurs), self-insurance basically means that you're assuming your own risk.

Self-insurance is basically a risk management approach that requires that you decide how much out-of-pocket loss you are willing to bear. Additionally, some companies decide to self-insure for certain types of losses, expecting that they aren't likely to happen.

A prime example of self-insurance is the deductible on your insurance policies. Your deductible represents the amount of financial costs you're willing to absorb in the event of a loss. It's the same principle. It just depends on the amount of tolerable deductible or length of time (waiting period) you are willing to accept.

Alternatively, some companies choose to set aside funds as if they are paying insurance premiums, so they'll have cash available in the event of a loss. These reserve funds serve to protect their operating cash flow if a disaster strikes.

Though these decisions are intentional, sometimes companies self-insure unintentionally. Unintentional self-insurance occurs when organizations aren't aware that there are exceptions to their coverage and it isn't until *after* the fact that they discover that the loss won't be covered after all. Of course, this only adds to the stress of the disaster!

Self-insurance is really only an appropriate option when you are able to reasonably predict the amount and timing of losses and have available reserves or other sources of funding in place to cover them. In any case, putting aside money in a cash reserve account to offset liquidity needs in an emergency makes sense.

COMMERCIAL INSURANCE

Although commercial insurance is certainly not the least expensive way to finance disaster-related losses, it does play several important roles in addressing cash flow challenges after tragedy strikes.

First, it assists in risk management by transferring the risk of loss away from you and onto an outside party. Obviously, this is good because you won't bear the entire cost of a disaster on your own.

Second, and probably most important, insurance can mitigate disaster-related cash flow impact by providing funds to repair or replace damaged property and equipment, to cover fixed costs during recovery (such as rent, utilities, and even payroll), to pay any additional costs of disaster recovery while trying to return to normal operations, or to replace lost revenue.

Although having insurance certainly doesn't ensure an organization's survival during disaster situations, it at least removes a portion of its financial obstacles by providing an infusion of cash when it's needed most. And in cases where a business has been completely wiped out and restarting isn't a viable option, insurance might at least allow the owner or owners to walk away with some equity.

A third intangible benefit of insurance during a disaster is having someone to rely on to help you through the recovery process. Both your insurance agent or broker and your insurance company have a wide variety of expertise and resources available to them that can help you prepare in advance, cope during a disaster, and get back to normal operations sooner.

BASIC TYPES OF INSURANCE

When talking about insurance, there are several different types of coverage available to consider. The most common types can be lumped into three basic categories: property insurance, automobile insurance, and liability insurance.

PROPERTY INSURANCE

Property insurance is the type of coverage that protects an organization from losses due to damage, total destruction, or theft of facilities and contents. Although the exact coverage varies by policy, this particular insurance typically doesn't cover earthquakes, floods, landslides, and terrorism.

For purposes of property insurance, business property often includes:

- Buildings and outbuildings (sheds, garages, and other structures not attached to the main facility)
- Sign, fences, and displays
- Equipment
- Furniture and fixtures
- Inventory and supplies
- Computers and other electronic equipment
- Phone systems
- Artwork and antiques

Again, depending on the policy, it may also include coverage for equipment breakdown, cleanup and removal of debris, or water damage.

Property can be insured for current cash value or replacement cost. Cash value reimburses you for the current value of the property or cost less depreciation, whereas replacement cost reimburses you for the cost to repair, replace, or rebuild the item at current prices.

Property insurance policies also come in two basic forms. An *All-Risk Policy* covers a wide range of losses typically faced by most businesses, except those specifically exempted in the policy. A *Peril-Specific Policy* covers only the risks specifically listed in the policy and are usually purchased for a specific need.

There are a couple of key tips and considerations to keep in mind with property insurance:

- You want to have a reasonably current assessment of your property's value

- Keep photos of (and copies of receipts for) valuable equipment, furniture, and artwork at an off-site location
- Have antiques and artwork appraised on a regular basis
- If you lease your facility, read your lease carefully to determine who is to provide property coverage on the building

AUTOMOBILE INSURANCE

Business auto insurance is similar to personal auto insurance, except that it's for vehicles owned by the business. This type of insurance covers costs to repair workplace damaged vehicles, also providing payments to third parties resulting from bodily injury or property damage for which the company is liable.

Many automobile policies include uninsured or underinsured motorist protection. This provides coverage for the insured if involved in an accident caused by an uninsured motorist.

LIABILITY INSURANCE

The third common type of insurance is liability insurance, and this coverage is designed to protect a business from potential or actual lawsuits. There are many forms of liability insurance.

General Liability. General liability insurance protects you from claims due to accidents, injuries, and negligence. It typically covers payments resulting from bodily injury or harm, medical expenses, property damage, libel and slander, false or misleading advertising, the cost of defending lawsuits, and settlement awards.

Product Liability. Product liability insurance protects companies that manufacture wholesale distributor and retail products, protecting them against losses resulting from defective products that cause injury or bodily harm.

Professional Liability. Also known as errors and omissions insurance, professional liability insurance is for businesses that provide services, and it protects against malpractice, errors, and negligence. This insurance also provides legal defense costs.

Directors and Officers Liability. Directors and officers liability insurance (sometimes referred to as D&O) protects past, present, and future directors and officers for damages arising out of alleged or actual wrongful acts. This includes actual or alleged errors, omissions, misstatements, misleading statements, or breaches of duty. Sometimes the coverage extends to employees.

General. A general liability policy provides coverage for compensatory damages (current and potential financial losses suffered by the injured party), general damages (nonmonetary losses suffered by the injured parties, such as pain and suffering), and punitive damages (additional penalties). It typically doesn't protect an organization against claims related to employment practices or operating a business vehicle.

Business Owners Policy. A business owners policy, or BOP, rolls multiple types of insurance into one policy. The benefit of this is that there's usually a discount for including multiple types of coverage. And, though it typically includes property insurance and liability protection, it may also include business interruption and automobile insurance.

Employment Practices. Employment practices is a type of liability insurance that covers damages that the employer is liable for if a violation of employee rights occurs. Coverage includes situations related to sexual harassment, wrongful termination of employees, failure to employ or promote, and race and gender lawsuits. It provides legal defense coverage, as well as paying any resulting judgment.

Workers' Compensation. Workers' compensation insurance provides coverage for medical care and a portion of lost wages for employees who are injured as a result of employment, regardless of who was at fault, and the agencies awarding benefits are often quite liberal. If an employee dies as a result of injuries sustained while working, the coverage provides compensation to his or her family. In addition, employers may also be subject to lawsuits from employees claiming that the employer did not take adequate steps to protect their employees during or after the disaster, which is where this insurance may come in.

Umbrella Policies. An umbrella policy is a type of liability insurance providing coverage over and above your organization's other liability coverage. Umbrella policies are designed to protect against excessive losses, usually when a judgment from general liability or auto liability exceeds the policy limits. An umbrella policy may also apply to professional liability insurance or employment practices liability insurance.

UNDERSTANDING YOUR COVERAGE

A key practice when doing business continuity planning is to review your insurance policies so that you better understand your coverage. When going through this process, it doesn't hurt to review them in detail *with your insurance agent or broker.*

Ask your agent or broker to explain your current coverage in a way that you can fully understand, and also ask what additional coverage he or she believes you might need. Here's a list of questions to take with you:

- What losses are covered by my policies?
- What are my policy limits?
- What are my deductibles? Under what conditions do these deductibles increase?
- What are the waiting periods for coverage?
- What losses are excluded or exempted from coverage?
- Are there any exceptions to the exemptions?
- What optional coverage do I have?
- What property and vehicles are listed on my policies?
- What are the agreed-on values for artwork and antiques?
- What recommendations do you have for additional coverage?
- What can I do to reduce the cost of my policies?
- What else do I need to know?

Liability insurance premiums are typically based on an estimate of the organization's sales and/or payroll. The cost can also be affected by the type of business and its related risks, any previous claims that have been filed, financial stability (or instability), state laws, and even the organization's approach to risk.

CONCEPTS TO KNOW

Certain insurance-related concepts require that more attention be paid to them than others because what your policies say in regard to these key areas can dramatically affect what happens with the insurance (and to your company) should a disaster occur.

DEDUCTIBLES

Deductibles are the amount of the damages you're responsible for paying before the insurance policy kicks in. Understand what these are and when they may change. (It's common for companies to carry a higher deductible on property policies for wind or hurricane damage because, though you *can* pay for a lower deductible, any damage sustained is usually quite extensive, thus expensive.)

As an example, let's say that your facility is insured for $500,000 and your normal deductible is 2 percent. After severe thunderstorms, you call your agent and claim a $15,000 loss. That's when your insurance agent advises you that there is a 5 percent wind deductible, so your loss doesn't exceed your policy deductible of $25,000.

HOME-BASED BUSINESS ISSUES

It's important to note that there are many misconceptions when it comes to ensuring a home business. For instance, many business owners make the mistake of believing that their homeowners' policy will cover both property and operations of their business.

However, most homeowners' policies have very low limits of coverage for business equipment and offer no liability protection. Therefore, if you operate a business out of your home, it's *crucial* that you discuss with your insurance agent or broker any additional coverage you may need.

PROXIMATE CAUSE

Although some risks may be excluded by your policy (such as floods after an earthquake), it's important to understand the concept of "proximate cause," because, in some cases, damage that appears to come from *one* cause may actually have come from another.

For instance, imagine that you own a restaurant and, as a result of a hurricane, you lose power and suffer flooding, spoiling your food inventory. The carrier initially denies the claim on the grounds that flood is an excluded risk. However, it's determined that the power loss occurred *before* the waters reached flood stage *and* that the spoilage would have occurred even if the flood had not. In this case, the carrier has to cover the loss.

FLOOD

Whether or not you are in a 100-year flood plain, you still run the risk of rising waters. In fact, 25 percent of all flood claims come from low to moderate risk areas.[1]

FEMA (Federal Emergency Management Agency) defines a flood as a general and temporary condition of partial or complete inundation of two or more acres of normally dry land area, or of two or more properties (at least one of which is yours) resulting from a(n):

- Overflow of inland or tidal waters;
- Unusual and rapid accumulation or runoff of surface waters from any source;
- Mudflow; and/or
- Collapse or subsidence of land along the shore of a lake or similar body of water as a result of erosion of undermining caused by waves or currents of water exceeding anticipated cyclical levels that result in a flood as defined above.[2]

Flood insurance is provided by FEMA and may be accessed by all insurance agents. It's also available nationwide, and not just in flood-prone areas.

Rates for flood insurance are standardized, which means that they're the same, regardless of the carrier. There *is* a 30-day waiting period for filing claims after signing up (except when flood insurance is obtained on a new mortgage) and claims *must* be filed within 30 days of a flood occurrence.

EARTHQUAKE

Earthquake coverage is not included in standard commercial property coverage, even though they've occurred in all 50 states. Many aren't severe, with the greatest amount of damage coming from sprinkler systems set off by tremors.

Like with flood insurance, earthquake insurance is also available nationwide, not just in earthquake-prone areas. However, unlike flood insurance, there is no single carrier and the rates vary. If you're in California, insurance is available through the California Earthquake Authority.

INFORMATION TECHNOLOGY

Information technology insurance is an optional rider providing coverage for business-related hardware, software, and data loss. Some policies extend coverage for hacking, denial of service attacks, and cyberfraud, while others include hard drive crashes, lightning strikes, and off-premises power interruptions.

Review your coverage for limits and make sure it restores lost data. Also, be aware that hardware losses are most often paid on depreciated value rather than on replacement cost and, when it comes to theft, many carriers restrict laptop theft to the United States only.

BUSINESS INCOME

Business income or business interruption insurance protects the income stream of a business as opposed to its property. The goal is to make the business "whole" after a disaster, providing coverage for lost revenue as well as covering any ongoing and additional expenses.

It's important to note that this particular coverage only protects you from risks covered by your commercial property insurance, and the loss must arise from a "covered cause." In other words, if your commercial property policy has exclusions for flood or earthquake, business interruption insurance also has exclusions for flood or earthquake. So be aware of the types of events you might face and determine whether to cover them as a separate endorsement under your business income policy.

Business interruption policies may be subject to a deductible and a waiting period, and the organization is typically required to restart operations as quickly as possible, either at the insured location or at an alternate location.

Claims typically require extensive documentation, such as income loss and expense calculations prepared and submitted by a CPA. For this reason, prior to a disaster, it's important to check with your CPA and ask whether his or her records are safeguarded so they'll be available after a disaster.

If you have a business owners package policy, business interruption insurance is often included. However, you may want to increase the limits of the standard coverage.

There are several types of optional business income insurance you can purchase. These include extended business income, contingent business interruption, and additional endorsements.

Extended business income coverage makes up the difference in lost revenue until business returns to normal revenue levels or for a certain specified period of time. For example, if a restaurant is destroyed by fire, once it reopens, it will take time for its normal customer base to return. Extended business income coverage can help fill this revenue gap.

Contingent business interruption coverage, also known as defendant property coverage, can be helpful for organizations highly dependent on one crucial supplier or a specific customer base as this insurance provides coverage for losses resulting from a third party's inability to complete a business transaction.

In order to apply, the third party *must* be unable to complete the transaction due to a covered loss. For example, if a plumbing parts supplier is dependent on Kohler for 40 percent of its inventory and the Kohler manufacturing facility is damaged by fire, which means that Kohler cannot deliver the inventory contingent, business interruption insurance would cover the supplier's lost revenue.

There are *additional endorsements* available for business interruption coverage, such as loss of utilities or loss of Internet access. If your business is highly vulnerable to any particular loss, you should discuss your options regarding business interruption endorsement.

Some key questions to ask your insurance agent or broker when buying interruption coverage include:

- What causes of loss are included?
- What is the waiting period before payments for lost income and extra expense begin?
- Is there a specific payment schedule?
- How long will the payments continue?
- Is there a time limit for returning to normal operations?
- What information and documentation will be required to submit a claim?

EXTENDED PERIOD OF INDEMNITY

Another concept you'll want to familiarize yourself with is your extended period of indemnity. This is the specified amount of time the policy will cover your income loss *after* any repairs have been completed.

For example, let's say your restaurant was damaged by fire and, after 10 months, you finally reopen. Your business income insurance technically ends at this time, but it will take several months for your customers to return and for you to return to prior operating capacity. The extended period of indemnity tells you whether you can claim any help for this period of time.

FILING AN INSURANCE CLAIM

Filing an insurance claim can be a long and tedious process, and one that typically requires significant documentation and analysis. However, you can expedite it by taking a few steps prior to and immediately after a loss.

For example, prior to facing a loss, take the time to document all of your property and assets. Include a description of each, the date of purchase, purchase price, the vendor you purchased it from, and, if possible, a current assessment of value. Support your documentation with pictures or video.

If you face a loss, immediately document it with pictures or video again. Include images of damaged items, as well as standing water. Inspect everything, even items that don't appear to be damaged. Especially after a flood, look for any evidence of leakage. Check foundations and walls for cracks or signs of a pest or rodent infestation. Turn on major systems like heat and air conditioning to see if they're working.

Next, you want to prevent continued damage, addressing safety concerns first. Begin cleanup and damage mitigation (such as draining water, lifting carpets, or removing spoiled inventory), and make temporary repairs. Remember to save receipts for repair services and supplies, and separate undamaged from damaged property. As long as you have video or photographs of the damage, you can begin cleanup and mitigation before contacting your insurance agent.

In the meantime, call your insurance agent or broker. Provide your policy number, loss location, cell phone number, and alternate contact numbers and confirm that the damage is covered under the terms of your policy. Inquire as to whether your claim will exceed your deductible.

Ask also about the time limit for filing the claim and determine whether you'll need to get estimates for repairs. The insurance carrier will likely assign an adjuster who should contact you within a few days. It is the adjuster who will provide you with a proof of loss form to file your claim.

The more organized you are, the better. Additionally, the more documentation you can provide, the easier it will be for the adjuster to prove your claim.

The initial steps an adjuster will take include reading your insurance policies and assessing the damage. That's why it is *critical* to fully understand the details of your policies up front in order to maximize your claim.

However, be aware that the insurance adjuster is not always right. That means that it's incumbent on *you* to know your policy and your coverage as the final settlement may be negotiated. If the claim is large or will take a long time to process, *you may request an early partial payment of claim or a schedule of claim payments.*

Dealing with damage to your business, equipment, and facilities after a disaster is difficult. It takes a significant amount of time and effort to get back up and running, and filing an insurance claim in addition can be overwhelming. In some cases, it may be beneficial to obtain help with the claims process from a public adjuster.

INSURANCE ADJUSTER VERSUS PUBLIC ADJUSTER

There are three people who can represent the interests of a policyholder during the claims process: an attorney, the insurance broker of record, and a public adjuster.

A public adjuster is essentially a private insurance claims adjuster who acts as an advocate for the policyholder in exchange for a fee. This is different from a claims adjuster as the claims adjuster works for the insurance company whereas the public adjuster works for the insured.

Public adjusters will manage and negotiate your insurance claim all the way from the initial assessment and cleanup through to repairs and rebuilding. They typically have significant experience with the insurance industry as many were previously employed by insurance companies and are generally licensed by the state or states in which they operate.

States manage the licensing through their insurance departments, and a majority require that public adjusters be tested, licensed, and bonded in order to practice their profession. Some are members of the National Association of Professional Insurance Adjusters (NAPIA).

NAPIA membership requires strict adherence to a set of standards and a code of ethics. It also provides certifications, including that of Certified Professional Public Insurance Adjuster (CPPA), a designation requiring a minimum of five years' experience and the passing of an examination to earn certification, and Senior Professional Public Adjuster (SPPA), which mandates a minimum of 10 years' experience and the passing of a rigid examination before earning "senior" certification. Both are required to continue the public adjuster's professional education and keep up with changes in the insurance industry.

Because of education and training, public adjusters are very familiar with how policies are written. They understand the uniqueness of the terminology (they know the difference between flood, partial flood, and wind-driven rain) and how to interpret exclusions and exceptions to the exclusions.

Other duties and responsibilities of an adjuster may include:

- Researching and substantiating damage to buildings and contents
- Documenting and substantiating additional expenses incurred
- Evaluating business interruption losses and extra expense claims
- Determining appropriate values for settling covered damages
- Preparing, documenting, and substantiating the claim
- Expediting the claim
- Coordinating all interactions with the insurance company
- Negotiating a settlement with the insurance company
- Reopening a previously filed claim if discrepancies are noted

Public adjusters generally charge a fee based on a percentage of the ultimate insurance settlement. This fee is paid by you, the policyholder, *not* the insurance company. The amount is deducted from the settlement payments paid by your insurance company, which means that, typically, the insurance company pays the settlement in two checks. One is issued to you and the other is issued jointly to you *and* the public adjuster.

The amount of the public adjuster's fee is negotiable and should be agreed on before signing a contract. Fees generally range from 10 to 25 percent, depending on the size of the claim and the amount of work involved. In theory though, because of their expertise, public adjusters may get you a higher settlement, ultimately offsetting the fee.

For instance, in 2004, I worked for a homebuilder in Florida. Between August 12 and September 25 of that year, Hurricanes Charley, Frances, Ivan, and Jeanne hit the state. In six weeks, we ended up with more than 250 builders risk insurance claims for houses under construction that were damaged, often multiple times. The insurance companies were overwhelmed and had to hire outside claims adjusters to handle all of their claims.

As the CFO, I was focused on getting the company back up and running, and I worked on removing damage and continuing construction. As the claims adjuster continued to ask for more and more records (historical detail and copies of invoices for each and every incurred cost in work-in-progress), it quickly became clear that I could either work on the insurance claim or work on the company. I chose to continue working on the company and hired a public adjuster to work on the claim.

After reading our policies carefully, the public adjuster determined that our coverage was for replacement cost, not historical cost, so there was no need to provide copies of invoices, only current pricing and quantities. His ability to interpret our coverage and change the claim from historical cost to replacement cost increased the size substantially. The fee for his services was expensive, 18 percent of the claim. However, the increase in the size of the claim well exceeded that amount.

If a disaster occurs and you're interested in hiring a public adjuster, some questions you want to ask include:

- What are your credentials, education, and training?
- How many years of experience do you have?
- What sort of claims have you worked on before?
- Are you licensed and, if so, in what state?
- Do you have local references?
- What are your fees?
- Will you handle all of the contact with the insurance companies or will I still be able to speak with them?
- Will you handle my claim personally?
- Will you be working with an attorney on my claim?

Navigating insurance claims isn't the easiest process. However, it can become slightly easier if you engage in predisaster financial planning, carry and understand basic types of insurance, learn more about the concepts most critical to *your* business, and understand the differences between insurance adjusters and public adjusters, as well as when hiring the latter may be worth the expense.

Questions to Ask Yourself

See if you can answer the following questions for your organization without referring to your policies.

1. What types of insurance coverage do you have?
2. For what types of disasters are you covered?
3. For what types of disasters are you *not* covered?
4. Under what conditions will your deductible increase?
5. Will your policies cover expenses beyond your normal business operations?
6. What is the difference between water damage caused by wind-driven rain and water damage caused by a flood?

NOTES

[1] "Low Risk Flood Zones," FEMA, https://www.fema.gov/faq-details/Low-Risk-Flood-Zones.

[2] "Flood or Flooding," FEMA, https://www.fema.gov/flood-or-flooding.

CHAPTER 12

Computer Systems: Disaster Prevention and Recovery

There's an old expression that "cash is king." But for many businesses, data is now more important. It is the lifeblood of the organization. Yet, unfortunately, many don't really understand the truly devastating impact of an IT disaster, thus they don't take the necessary steps to protect themselves.

Have you ever been working on a report or tax return when the lights flickered and you lost 15 minutes of your work? How frustrating was that? And when you lose an hour of it? The frustration and cost to recover your information increases dramatically.

The concern for technology threats is evident in the AICPA's 2013 North America Top Technology Initiatives Survey, with the top 10 concerns for CPAs in the United States being:

1. Managing and retaining data
2. Securing the IT environment
3. Managing IT risk and compliance
4. Ensuring privacy
5. Managing system implementations
6. Preventing and responding to computer fraud
7. Enabling decision support and analytics
8. Governing and managing IT investment/spending
9. Leveraging emerging technologies
10. Managing vendors and service providers

Ernst & Young interviewed 1,900 C-suite professionals and published their findings in its *Under Cyber Attack: EY's Global Information Security Survey 2013*. Cyberrisks and threats were top concerns for 62 percent of the respondents. So it's safe to say that IT issues are feared disasters, and we have good reason to be afraid.

In January 2014, someone hacked into the Chamber of Commerce's system in Bennington, Vermont,[1] installed ransomware, and held the server hostage, asking for a $400 payment. Although the directors attempted to pay the money, they were unsuccessful and lost everything.

In the IT world, it's often said: "There are two types of companies in this world. Those that have been breached, and those that are going to be breached." In fact, some IT professionals believe that data breaches are just a fact of life, on par with taxes and death. Statistics appear to prove it.

Storagecraft[2] reports that 140,000 hard drives crash every week, yet, *only 23 percent of companies back up their data daily*. Of those, only 66 percent test their tape backups. When they *do* test them, 77 percent have found failures. According to research conducted by the National Cyber Security Alliance, almost 50 percent of small and medium businesses have experienced a cyberattack, and 60 percent of small and medium businesses that experience a significant data loss will go out of business.[3]

Then there are the issues from outside attacks. Highlights from Symantec's 2017 Internet Security Threat Report[4] indicate:

- In 2016 there were 15 data breaches that exposed more than 10 million identities each.
- In the past eight years, 7.1 billion identities have been exposed in data breaches.
- Fifty-three percent of all e-mail is spam.
- One out of every 131 e-mails contains malware.
- Over the past three years thieves stole $3 billion of business e-mail phishing scams.
- Ransomware attacks have increased by 36 percent with more than 100 new malware varieties.
- The average ransom demanded in ransomware attacks increased by 366 percent in one year.
- Seventy-six percent of websites scanned contain vulnerabilities that can be leveraged by fraudsters.
- An Internet of Things (IoT) device, such as a smart TV, smart thermostat, or cable modem, can be attacked and taken over in two minutes.

Information Age reported the following statistics in 2017:

- A 38 percent increase in reported cybersecurity incidents
- Fifty percent of small and midsize organizations suffering at least one cyberattack in the past 12 months.

There are many noteworthy examples of technology failures, including website failures, software failures, and data breaches.

For instance, in December 2013, Target was the victim of a malicious data breach. Hackers stole the debit and credit card information of 40 million customers, also taking the e-mail and mailing addresses of an additional 70 million customers. *USA Today* reported that costs associated with that breach were "between $400 million and $450 million."[5]

There were also several instances of software failure that year. In one case, United Airlines had pricing issues on its website, selling some flights for only a dollar. Fortunately for their customers, they chose to honor those transactions.

Walmart's customers weren't so happy when, in October 2013, the company website listed computer monitor projectors for as little as $8.99. They chose to take the opposite approach of United and refused to honor these partner deals, canceling the purchases, and angering many customers.

The largest ever reported breach occurred at Yahoo with the disclosure of three billion e-mail accounts—every account that existed at the time. Although the breach occurred in 2013, it was not discovered and disclosed for more than three years. The breach reduced the selling price of Yahoo to Verizon by $350 million. And to this day, Yahoo does not know how the hack was accomplished.

In 2017, Equifax experienced a data breach that exposed 148 million records, which is approximately 61 percent of all adults in the United States. The disclosed data included credit card, driver's license numbers, Social Security numbers, date of birth, phone numbers, and e-mail addresses. The enormous breach was the result of one outward-facing server with outdated software. The attack went on for 76 days before it was noticed. And then, Equifax waited six weeks before reporting the breach. As of the end of 2017, the costs related to the breach are $439 million and estimated to ultimately reach $600 million. In addition, Equifax has budgeted another $200 million to increase their security. Data breaches are not cheap, one server with outdated software will cost Equifax more than $800 million.

In the first half of 2018, 182 million records were exposed in the 10 largest reported breaches. The majority of the exposed records came from UnderArmour, where 150 million records were exposed.[6] UnderArmour was extremely responsive and notified users four days after discovering the breach.

Sadly, 50 percent of companies that lost their data for 10 days or more filed for bankruptcy immediately after the data disaster and 93 percent filed for bankruptcy within a year.[7] To make matters worse, many business owners mistakenly assume that cyberattacks only occur to large companies, but the numbers suggest that isn't the case.

According to the U.S. House Small Business Subcommittee on Health and Technology, 20 percent of all cyberattacks actually impact small businesses. In addition, 63 percent of them are on companies with less than 100 employees. What's scarier yet is that Gartner Group reports that 50 percent of small and medium-size businesses that manage their own network will be hacked and *won't ever know it*.

Look at it this way: Only 39 percent of companies review their IT disaster plans annually, but how many hackers review their approaches daily? It is *absolutely critical* for your organization to have a plan in place to protect your technology systems and respond in the case of a disaster.

CAUSES AND COSTS OF IT DISASTERS

One reason IT disasters are so hard to prevent is that they can be created by so many different events. These include:

- Server failures
- Hard drive crash
- Power outages
- Service provider failures
- Software glitches or failure
- Malicious virus
- Ransomware (a type of malware that freezes access to all of your computer's files)
- Natural disaster (such as flooding or earthquake)
- Employee sabotage (or theft)
- Human error

Although the possible causes are many, one thing is for sure. These types of issues, regardless of the cause, are often extremely costly. Companies lose money due to downtime, data loss, data corruption, and repair. There are also costs to restore software, restore hardware, patch security holes, and perform data recovery.

Add that to the cost of credit monitoring, costs associated with loss of credibility and customer trust, and lost revenue when customers cannot do business with you and the numbers just go up. Of course, then there are penalties for violating contracts with partners, suppliers, and distributors, and legal costs of compliance. The list goes on and on.

According to Symantec,[8] IT outages cost the typical small business $3,000 a day, and the median cost of downtime is $12,500. Some companies wind up paying much more.

Sony PlayStation's breach of 77 million records cost them $171 million, and on August 1, 2012, Knight Capital experienced a disaster that lasted only 45 minutes, yet cost the company $440 million (four times their 2011 net income) when they installed new trading software and a glitch caused the firm's computers to buy and sell millions of shares of stocks incorrectly, dropping capital stock 63 percent by the end of the day. Ultimately, to cover the losses, 70 percent of the company had to be sold.

According to the Business Continuity Institute's *Horizon Scan 2014 Survey Report*,[9] if you look at that year's top 10 threats to business continuity, the first three are IT-related: (1) unplanned IT and telecom outages, (2) data breach, and (3) cyberattack. Meanwhile, McAfee Labs 2014 Threat Predictions report[10] forecasted that:

- As mobile malware attacks are increasing at a far greater rate than those on PCs (rising by 33 percent in the last half of 2013), this trend will most likely continue.
- Virtual currencies will be used to make ransomware payments.
- Online attacks by criminal gangs will increase in number and strength.
- Platform attacks against social websites, such as Facebook, Twitter, LinkedIn, and Instagram will continue to grow.
- PC and server attacks will continue to leverage weaknesses in operating systems and website programming.

- The adoption of "big data" security analytics will be necessary to meet detection and performance requirements.
- As cloud-based systems become more widely used, cybercriminals will attack those data repositories.

IT DISASTER PREVENTION

We've all said, "You get what you pay for," and this is especially true when it comes to today's technology because buying cheap equipment leaves you vulnerable to hardware failures. Sure, a $300 server may sound like a deal compared to one that costs $3,000, but the cheaper version likely won't be as reliable or last as long.

Another factor to consider when it comes to preventing IT disasters is to be consistent in your equipment purchases. Hardware compatibility becomes a major issue when you purchase different brands, such as Dell versus Apple verus Toshiba. In addition, too many brands make it difficult for your IT department to become experts in any one type of hardware.

Software is another area where consistency is helpful as data integrity becomes an issue when you're using different versions of the same program. For example, if some of your employees use Microsoft Office 2010 and some use Microsoft Office 2013, you're likely to experience problems.

It also helps to update software programs on a regular basis on the server level *and* at the user level. This includes PCs, laptops, and tablets because, although it's easy for your IT department to schedule updates to the software on the server, it can be much more difficult to push updates to users.

You may even decide to prevent users from installing their own updates without permission from your IT department. Often, viruses and malware can be installed on a computer system when the user mistakes them for normal software updates.

Though the least expensive way to deal with an IT disaster is to spend money on prevention, one of the most overlooked considerations is the facilities housing your systems. Many large organizations have dedicated server rooms, but a lot of small and medium-size enterprises do not.

Often, servers are an afterthought, kept in a spare closet and stored among other materials and supplies, greatly increasing the risk of hardware failure. The room may not be dusted on a regular basis, increasing the risk of fire. There may be too many items plugged into a single outlet or power strip. There may be cables and loose wires creating a tripping hazard. There may be many pieces of equipment, some new and currently being used, some old and unused. There may be cardboard boxes of old supplies making it difficult to move around the room and access the equipment. And, worst of all, nothing is labeled. So when something fails, it is extremely hard to identify and fix the issue.

Okay, maybe it isn't that bad, but if it's not neat and orderly, this is something you should work to remedy immediately. The first step in protecting your onsite servers and helping to prevent hardware failure is to ensure the facilities housing your systems are clean, regularly dusted, and free of pests.

Speaking of pests, in 1945, computer scientist Grace Hopper coined the expression "computer bug" when she discovered that a moth had short-circuited the Harvard Mark II computer she was working on. Other animal-related IT disasters have occurred due to rats chewing on wires or nesting inside a server, spiders spinning webs inside a server, or hatching baby spiders inside the CD drive.

Your housing facilities should also be:

- Adequately ventilated
- Adequately air-conditioned
- Wired professionally
- The servers plugged into battery backup systems (uninterrupted power supplies)

Servers and battery backup systems should be tested quarterly if you aren't replacing your batteries yearly. Battery backups allow you time to shut down your system in the event of a power outage and prevent fires from electrical surges.

Many people mistakenly assume that a power strip is also a surge protector; but often power strips just provide additional outlets (ultimately overloading the electrical system). And just because a strip has six outlets it doesn't mean that the power strip is rated to be running six different appliances. When a power strip is overloaded (even if it is a surge-protector), both the power strip and the attached equipment can melt or catch fire.

For security purposes, your server room should be kept locked and have limited access because one of the simplest things a company can do to prevent an IT breach is to mandate access controls. Take the time to set up proper access limitations for both administrative and nonadministrative employees (especially when employees are using personal devices to access company data) to mitigate this top IT threat. Install surveillance cameras and check them regularly to make sure the cameras are working.

Layering security is also a good approach, but it's not necessary to require high-level security for every application. An employee's initial login should require the strongest of passwords, with an additional password required to access your accounting system. It may not be necessary to require a third level of passwords for individual portions to the accounting system though, such as accounts receivable, so you want to apply the appropriate level of security based on the confidentiality of the system.

When it comes to passwords, employees may love to hate them, but they are in fact a very effective control. Here's a list of 10 things you should *never* do with passwords:

1. **DON'T use common dictionary words** in *any* language; for instance, don't use *monkey*, *computer*, *password*, or *buenos dias*.
2. **DON'T spell common words backwards**, such as *retupmoc* or *drowssap*.
3. **DON'T use sequential numbers**, like *12345* or *9876*.
4. **DON'T use personal information**; stay away from using your name, a pet's name, or your favorite sports team.
5. **DON'T substitute a similar number or symbol** for an alphabetic character; *p@ssword* should never be a password.
6. **DON'T use a common word with just a number added**; don't use *Tommy1* or *Apple5*.
7. **DON'T use a string of identical characters or numbers**; *BBBBB* and *111111* should never be used.

8. **DON'T use your login ID** as your password; these two should always be different.
9. **DON'T write your password down and keep it in all the typical places**; don't keep your password on a sticky note on your monitor, underneath your keyboard, in a file labeled "passwords," or on the last page of your calendar.
10. **DON'T share your password** with anybody else; your password should be known by you and you only.

Now, if those are all the things you're *not* supposed to do, what *can* you do to develop a strong password and maintain your security?

Ideally, to create a strong password, you want to:

- Use a minimum of 10 characters, but even longer is better.
- Also, make your password a combination of alphabetic, numeric, and special characters.
- Use a combination of lowercase and capital letters.
- Set different passwords for different types of log-ins. (For example, you want to use different passwords for banking sites, social media, and e-mail accounts.)
- Most important, you want to change your most critical passwords on a regular basis.

LAPTOP AND CELL PHONE PROTECTION

Laptop theft is a significant threat to individuals and organizations alike. Ponemon Institute reports that 12,000 are lost weekly, with the average cost to an organization for *just one of them* right around $49,246.[11] And only 7 percent of stolen devices are recovered.

According to some estimates, one out of every 10 stolen laptops is taken at an airport. In one commonly used method, two criminals position themselves in front of a victim while in line for TSA luggage screening. The first one goes through the metal detector while the second delays the victim by distracting security personnel, often by intentionally placing metal objects in various pockets. Meanwhile, the victim's luggage and laptop pass through the screener and, while the victim is stuck behind the second criminal whose pockets are being emptied, the first criminal steals the laptop as it comes off the conveyer belt.

A frequently overlooked step to protecting laptops is simply educating employees on laptop safety. They should be regularly trained and updated on how to protect themselves and their data, particularly when traveling. Steps they can be instructed to take include:

- Always keep your laptop with you. In particular, don't leave it at a restaurant table, behind a chair, or in your car.
- Use a security cable and lock when leaving it at the office or in a hotel room.
- Write down the laptop's serial number, make, and model. You'll need it if you ever have to report a theft.
- Back up your files regularly and test the backup.
- Encrypt your hard drive. If your laptop is stolen, this will minimize the data loss.
- Consider installing a tracking device or software.
- Install utility software that will notify the police if it is stolen.
- Install antivirus software.
- Install a firewall.
- Remove unnecessary data.
- Set an idle time-out, requiring the use of your password to log back in.
- Use a strong password.
- Don't leave a copy of the password in the carrying case or taped to your laptop.
- Use a screen guard to prevent strangers from seeing what you're working on.
- Keep software updated, especially for security patches.
- Customize the appearance of your laptop and carrying case to make them distinctive.
- Be careful when using Wi-Fi networks.
- Store your data in a cloud so that if your laptop *is* stolen or broken, you still have access to your data.
- Insure your laptop.

Sadly, cell phones don't fare any better as they're most frequently stolen at airports, in mass transit, and from cars. According to *Time* magazine, cell phone theft in major cities has become an epidemic. In New York City, for example, there was a 40 percent increase in cell phone theft in 2012, and it's estimated that, in 2013, 3.1 million were taken from their owners.[12]

In Chicago, cell phone theft has become the modern-day purse snatching. Criminals are targeting victims who are using their cell phones on the subway. It goes something like this: The person is involved in a phone call and not paying attention. Just as the subway doors are opening at a stop, the criminal grabs the victim's phone, jumps off the train, and disappears into the crowd.

The issue for organizations is that mobile phones contain a great deal of confidential information. This puts their contacts, e-mail, Internet credentials, usernames and passwords, business applications, and/or mobile payment information at risk if the phone is accessed.

Plus, we often get distracted when using our phones, making ourselves easy targets for thieves. That's why it's a good idea to hold your phone tightly, potentially even using two hands, especially while in public places. It may look strange, but wouldn't you rather look silly than be robbed of your phone?

Other steps you can take to protect your cell phone include:

- Never let it out of your sight, paying special attention to never leave it unaccompanied on the restaurant table or in your car.
- Write down your phone's number, make, model, serial number, and PIN (or security lock code).
- Lock your phone using a security code or PIN feature.
- Install antitheft software that will remotely locate your lost device and, if necessary, destroy all of its data.
- Install antivirus software.
- When carrying your phone, make it difficult to access. If it's easy for *you* to reach, it's easy for criminals to reach.
- Back up your data and photos regularly.

If your phone *is* stolen, report it immediately to police and your carrier. Your carrier can blacklist it and prevent anyone from making calls. Also, immediately activate any tracking and remote device management software.

NETWORK SECURITY

One major concern of businesses is that their network will infect a client with a virus or be used by hackers to gain unauthorized access to information. The risk of either of these happening can be lessened by taking proactive steps, such as:

- Installing a firewall
- Putting virus protection on all of your company's computers and mobile devices
- Using antispam software
- Establishing a VPN for remote access
- Setting appropriate administrator rights and responsibilities
- Placing restrictions on downloads and upgrades
- Conducting employee training

Additionally, all of your files need to be backed up. This means that files used by employees should *always* be saved on your server, not on their local desktop or laptop. A good backup system is off-site, automatic, uses an external hard drive (rather than a tape or CD system), and includes backup of software applications.

Another preventative step is to develop IT security policies and procedures, sharing these with all employees via regular training sessions so they understand what you expect in this regard. An effective IT security policy will cover:

- Confidentiality of client records
- Transmission of data
- Computer security
- Wireless transmissions
- Remote access
- Computer backup
- Credit card information

- File retention
- File destruction

One of the newest risks in today's IT environment involves BYOD, short for "bring your own device." Many employees prefer to use their personal devices—such as laptops, tablets, or cell phones—in lieu of those provided by the employer. Symantec reports that the average employee connects 2.8 devices to an employer network *every single day*.

Whether you currently allow employees to BYOD or you're considering it as a viable business option, ask yourself these questions first:

- Is there an assumption of privacy?
- How will you address confidentiality of proprietary information?
- Who pays for the services?
- How will you address software compatibility?
- What happens if the device is broken or lost?
- What happens when the employee leaves?
- What security policies will you require?

Keep in mind that, although security is definitely an issue, creating a policy that is too restrictive won't necessarily help keep your data secure. Further, the Gartner Group estimates that 20 percent of BYOD programs will fail because they are too restrictive and difficult to follow, which makes finding a happy compromise the best solution.

To establish a good BYOD policy, you want to define policies that employees can live with. Make a clear separation between work and personal lives when it comes to devices. Choose apps that don't directly store data. Fully explain the risks of BYOD; and, finally, communicate your policy to your employees on paper and in person.

OPERATING IN THE "CLOUD"

The "cloud" refers to the use of web-based applications that provide access to data from any location at any time, as long as there's a working Internet connection. Some companies prefer them because they generally incur lower hardware and maintenance costs as they're paid for on a pay-as-you-go basis or with per-user fees.

Although the cloud does offer some advantages, there are some risks associated with this type of application as well. For instance, there can be issues with security, both physical security of the hardware and security of the data. There's also a potential for downtime and questionable availability of customer support.

The speed and bandwidth required for access to cloud-based applications can sometimes cause issues as well. Legally, there is the need for disclosure to clients, whether required by the IRS and/or by the AICPA Ethics Ruling No. 112.

According to a Ponemon Institute study, the majority of cloud-computing providers believe it is *the customer's responsibility* to secure the cloud. Additionally, the provider's systems were often *not* evaluated for security prior to deployment, did *not* have dedicated security personnel, and the user had no idea what was being done to protect their data.

In order to compensate for some of these risks, organizations should request disclosure from the provider. Ask about their security programs and policies, their disaster recovery plans, their employee hiring policies, and their liability insurance policies. You also want to request third-party monitoring of their security and evaluate their financial stability. The more you protect yourself in the beginning by taking these types of actions, the safer your data becomes.

When using a cloud provider, your contract with them should address confidentiality as they shouldn't be able to make any unauthorized disclosures, and there should be no unauthorized use of data by them. It should also state who will bear financial responsibility if either of these occur. Include a Right-to-Audit clause where you, the customer, can review their security policies and procedures. You also want to review their SOC-2, Type 2 Report.

Technically, an SOC report is the result of an examination engagement undertaken by an external auditor to report on the controls at an organization that provides services to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting. Put simply, it's a report that tells you whether your provider takes their internal controls seriously.

There are three types of SOC reports, and, to make it even more complex, each report can have different types. For instance, an SOC 1 report covers the service organization's internal control system, and there are two versions of it. Type 1 is a report on management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

Type 2, on the other hand, is *also* a report on management's description of the service organization's system and the suitability of the design, but it also addresses the operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period. This report is more expensive because it covers not only the design but also the usage of the internal controls.

An SOC 2 report is slightly more comprehensive and covers the specific controls at a service organization relevant to security, availability, processing integrity, confidentiality, and privacy. It's essentially intended to provide assurance about the controls that affect these issues and, like an SOC 1, comes in two types. Type 1 only addresses the design of the controls, but Type 2 addresses both the design and the effectiveness of the controls.

Finally, SOC 3 reports are designed to meet the needs of users who need assurance about the controls at a service organization, but at a more general level. These reports are general use reports that can be freely distributed or posted on a website using an authorized seal of approval.

To be most comfortable with the controls of a service organization you intend to use, you should request a SOC 2, Type 2 report. (If you'd like more information about SOC reports, it's available on the AICPA website (https://www.aicpa.org/InterestAreas/InformationTechnology/), where you can download the brochure, "Service Organization Controls."

CREATING AN IT DISASTER RECOVERY PLAN

When creating an IT disaster recovery plan, one of the first things an organization has to define is the difference between an "inconvenience" and a “disaster.” These definitions may vary between departments and between employee roles.

For example, if your customer service employees can’t access your customer relationship management (CRM) software for 15 minutes, the impact will be immediate if they have no other way to answer customer’s questions. However, if your accounting department can’t access general ledger software for 15 minutes, it’s more of an annoyance.

Another consideration is recovery time. How quickly does each system need to get back up and running? Again, this may vary by department, system, or employee role. Customer service software may have a quicker recovery time, for instance, than accounting software.

Don’t forget to consider regulatory requirements because many industries are subject to specific regulations covering data security. These regulations can be at both the federal and state level, and noncompliance can result in fines, loss of business license, or even jail time.

Table 12.1 is a list of some of the more applicable federal data retention regulations (*Appendix H includes a list of many of the U.S. privacy laws, for your convenience*).

When it comes to the software systems you use, not all of the systems are created equal and not all of them need to be running all the time. So, after identifying all of the systems running on your server and mobile devices, the next step is to rank them in terms of criticality as those are the ones you want to protect most. For instance, CRM and accounting software are more critical elements of Microsoft Office programs, such as Excel and PowerPoint.

Not all data is critical either, so you want to identify what is, what is archival (historical copies), and what is useless. During this process, don’t forget to include data that is not stored centrally because when employees use laptops, they sometimes mistakenly store files locally rather than on the server.

Your organization also needs to consider how employees might access their programs and data if they couldn’t come into work or if the power goes out at your facility. (When doing this, be careful not to confuse accessibility and availability with disaster recovery.)

Table 12.1 Common Federal Data Retention Regulations

Regulation	Summary
HIPAA	Organizations must ensure data privacy and restricted access while information is being transmitted and in storage.
FTC Red Flags Rule	Many organizations are required to implement a written Identity Theft Prevention Program designed to detect the warning signs of identity theft in their day-to-day operations.
Subtitle D of Title XIII of the ARRA	Additional requirements supplement the HIPAA Privacy and Security Rules.
Federal Information Security Management Act (FISMA)	Federal agencies, and those providing services on their behalf, are required to develop, document, and implement security programs for IT systems and store the data on U.S. soil.
Gramm-Leach-Bliley Act (GLBA)	Provisions are included to protect consumers' personal financial information held by financial institutions and higher education organizations.
Payment Card Industry Data Security Standards	Information is covered related to credit card holder data as defined by the Payment Card Industry Data Security Standards.
Sarbanes-Oxley Act	Subject companies must create accounting systems with easily verifiable and traceable source documents; revisions to accounting software must be fully documented.

One location-based solution is to have a "hot site." There are vendors that will provide fully configured data centers with commonly used hardware and software programs. In some cases, applications, data streams, and data security services can also be hosted and managed by these vendors.

Creating an IT disaster recovery plan is very similar to creating a business continuity plan in that data recovery plans are not just an IT responsibility. That's why it's important to involve everyone in the organization in the development of IT-related security policies.

Disaster recovery plans should address four basic IT protections: data protection, system recovery, people, and processes. When it comes to data protection, your data needs to be backed up and secured at an off-site location. System recovery in the plan will address the platforms, servers, operating systems, software, networks, and storage that you'll use to recover your applications.

Because people will be performing the work, it's important to ensure that they have operational places to work from with the right equipment to enable them to do their jobs when trying to restore your IT system. When developing an effective IT disaster recovery plan, the steps can be summed up as follows:

Step 1: Assess your risks.

Step 2: Test your systems for vulnerabilities and risks; it's better that you find out where the weaknesses are *before* somebody outside your organization exploits them.

Step 3: Develop recovery strategies, addressing the length of disruption (24 hours? 72 hours? five days or more?), type of disruption (single system? branch location? entire network?), type of disaster (power outage? virus? fire?), and assignment of personnel.

Step 4: Test the recovery plan; the last thing you want to find out is that the backups that you're relying on will not restore (*a sample IT backup and testing form is located in Appendix I*).

Step 5: Communicate the plan to all employees.

Step 6: Update the plan regularly (at least every quarter).

Though you may be tempted to skip Step 4 and not test your recovery plan, to do so could be catastrophic. For example, prior to Superstorm Sandy, the manager of a marina contacted her IT consultant to confirm that her systems were being backed up. She was told that all of the company's data was on a schedule to be backed up nightly, but, after the storm, she learned that the backup system had not run for two entire months.

Many organizations also choose to create a separate breach plan to address hacking, data loss, and server extortion. If you're interested in creating a separate breach plan, the process looks like this:

Step 1: Identify, locate, and map digital assets.

Step 2: Identify risks and potential types of breaches.

Step 3: Develop response plans for mitigation and correction.

Step 4: Develop a communication plan.

Step 5: Update regularly.

CYBER INSURANCE

While cyber insurance (sometimes referred to as cybersecurity insurance) will obviously not help with prevention of a cyberattack, it can at least help mitigate the losses related to data recovery. Your property insurance policy will cover your physical computer equipment, but how about the costs of downtime and data recovery?

Cyber insurance can include many types of coverage. For instance, a data breach of privacy crisis management coverage steps in on issues related to managing an investigation, data recovery and remediation, third-party notification, call management, credit monitoring, legal defense costs, legal damage awards, and regulatory fines. Multimedia liability covers website defacement and intellectual property rights infringement, and extortion liability covers costs associated with negotiating with extortionists, ransom fees, and data recovery.

Before buying cyber insurance, assess your IT systems. Take an inventory of all of your computer equipment, map out your network (*a sample network map is provided in Appendix J*), identify all software programs, and document your current security procedures.

Next, consider your desired coverage. Start by identifying what costs you'd like to have covered and what incidents you want to be covered for, brainstorming with your IT department. Together, create a list of all the types of incidents that may occur, then create a list of all the potential costs and expenses related to those incidents.

The third step is to talk to your broker and discuss your cyber insurance options. Ideally, you want someone who has experience in IT coverage, which may mean finding a specialist broker.

No two businesses are the same and, in cybersecurity, risks are changing all the time. So, there are additional considerations when reviewing your potential policy, including:

- Will you have to undertake a security risk review?
- What steps that, if taken, will reduce or limit the risks?

- Do all portable media or computing devices need to be encrypted as a mark?
- What assistance is provided to improve your IT security?
- What is the impact on future premiums if you make a claim?
- Are malicious acts by employees covered?
- What is the maximum limit of coverage?
- Are limits for expenses grouped together?
- What legal defense costs are covered?
- What is the time period for discovering, reporting, and covering a breach?

Questions to Ask Yourself

1. How would your organization be affected if you could not access your server and your data for 24 hours?
2. How would you conduct your business in regard to data access if you couldn't come into work?
3. What costs would you incur if you lost half of your customer data? What if you lost it all?

NOTES

1. "Hackers Holding Computers Hostage," Donna Leger (May 15, 2014), *USA Today*.
2. "Infographic: The High Cost of IT Disaster," Casey Morgan (October 29, 2013), Storagecraft; www.storagecraft.com/blog/infographic-high-cost-disaster.
3. "60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think)," Thomas Koulopoulos, Inc.com (May 11, 2017).
4. "Symantec 2017 Internet Security Threat Report, Volume 22," Symantec Security Response Publications (2017), https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.
5. "Data Breach Takes Toll on Target Profit," Bruce Horovitz, *USA Today*, (February 26, 2014).
6. "The 10 Largest Data Security Breaches of 2018 (So Far)," Michael Novinson, *CRN* (July 31, 2018).

7. National Archives and Records Administration, Washington, DC.
8. "SMBs Not Prepared for Disasters, Don't Act Until It's Too Late," Symantec (January 11, 2011), www.symantec.com/about/news/release/article.jsp?prid=20110111_01.
9. "Horizon Scan 2014: Survey Report," Business Continuity Institute (2014), www.bsigroup.com/Documents/iso-22301/resources/BSI-ISO-22301-Horizon-Scan-2014-UK-EN.pdf.
10. "McAfee Labs 2014 Threats Predictions," McAfee Labs (2013), www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf.
11. *The Billion Dollar Lost Laptop Problem*, Ponemon Institute (October 31, 2010), www.intel.com/content/dam/doc/white-paper/enterprise-security-the-billion-dollar-lost-laptop-problem-paper.pdf.
12. "Law Enforcement Sounds Alarm on Cell Phone Theft Epidemic," Michael Scherer, *Time* (March 25, 2013), http://swampland.time.com/2013/03/25/law-enforcement-sounds-alarm-on-cell-phone-theft-epidemic/.

CHAPTER 13

Special Disaster Issues

Though we've already talked about the fact that disasters can be environmental, biological, deliberate attacks (man-made events), utility disruptions, equipment-based, attacks on information technology, economic, or some other type, there are often some disasters that business owners tend to have more questions about than others. Let's talk about those now.

POWER OUTAGE

Power outages can be frustrating because you don't know how long they'll last. It could be an hour, a day, or a week. To be better prepared if this type of issue occurs at your business, there are a few actions you can take. These include:

- Check auxiliary lighting and exit lights to make sure they're functioning.
- Provide a stock of extra flashlights and batteries, distributed throughout the facility.
- Assign a contact person to contact the utility company and provide updates to employees.
- Prepare a communications plan so employees will know how to stay updated.
- Stock up on extra gallon jugs of water to allow employees to wash their hands and flush toilets.
- If you plan to use a generator, stock up on fuel and test it under realistic conditions. (Testing its ability to support one floor is not the same as having three floors draw on power at the same time.)
- Install carbon monoxide alarms.

Once a power outage actually happens, there are a few additional things you can do to minimize any possible damages. These include powering down computer equipment (assuming it's on battery backup and still has the ability) and unplugging all equipment not plugged into a surge protector.

Leave one light turned on so you will know when the power comes back on, and cancel or reduce employees' travel requirements if traffic lights are out. If you're using a generator, ensure that it's well ventilated.

Avoid any downed power lines and report the outage to the utility company. Finally, once the power does come back on, throw away any food in lunchroom refrigerators that may have become too warm. ("When in doubt, throw it out!")

Speaking of power, it's important to remember that you do have some control over your energy usage during times when power is still on. During periods of high-energy consumption, such as a heat wave or a cold snap, for instance, steps can always be taken to conserve energy and possibly reduce outages due to the lessened energy demand.

This means turning off all nonessential lights, computers, and equipment, and installing motion detectors in areas where lights don't need to be constantly on (bathrooms, lunchroom, infrequently used storerooms, etc.). Adjust your thermostats when employees aren't in the buildings, such as at night and on the weekends. Replace incandescent light bulbs with energy-efficient fluorescent bulbs.

FIRE

Fire is one of the most destructive hazards for a business. It not only disrupts your operations, but it also forces you to find alternate facilities for employees and production. Thus, the best-case scenario is to protect your organization from fires by removing the very hazards that tend to create fires (or enable fires to engulf your whole facility). How?

- Contact your local fire department for a fire hazard inspection.
- Install smoke detectors and schedule battery replacement twice a year.
- Periodically test alarms. Test the sprinkler systems while you're at it.
- Make sure the numbers of your street address are easily visible from the road.
- Contact your insurance company to get recommendations for fire prevention and protection measures.

- Ensure flammable materials and liquids aren't stored near fuse boxes or natural gas lines.
- Remove fire hazards, such as stored paper.
- Install GFCI outlets anywhere water is near (bathrooms, manufacturing areas, kitchens, and pantry areas).
- Establish, mark, and post evacuation routes.
- Regularly test emergency lighting and exit lights to make sure they function properly.
- Educate employees on fire prevention, fire containment, and evacuation procedures.
- Conduct fire drills and establish congregation areas to account for all employees.
- Have fire extinguishing equipment inspected annually.
- Train appropriate employees on the use of fire extinguishing equipment.
- Make sure you have the appropriate number and type of fire extinguishing equipment.
- Establish procedures for the safe handling and disposal of flammable materials.
- Mark all utility shutoffs so these utilities can be secured quickly.

Should a fire occur, your response is critical. Of course, the first step is to evacuate the building. Don't use elevators to exit, and call 911 immediately! Once outside and away from the threat, take attendance to account for all employees (and visitors), and wait for the fire department to arrive.

HAZARDOUS MATERIALS SPILL

A hazardous materials spill can pose a significant threat to your personnel and property. If it's bad enough, it can even affect the entire neighborhood.

If your organization works with hazardous materials, make sure you're aware of and in compliance with all applicable local, state, and federal laws regarding their use, storage, and handling. You should also be aware of the hazardous materials that are used by other businesses in your neighborhood, as well as those that are transported on nearby roads, railways, and waterways.

To prepare for a potential hazardous materials spill:

- Identify and label all hazardous materials used and stored in your facilities.
- Prominently display all Materials Safety Data Sheets (MSDS) for the identified materials.
- Ask your local fire department and insurance company for assistance in developing appropriate response procedures.
- Train employees in the use, handling, and storage of hazardous materials.
- Train employees to recognize and properly report a spill of hazardous materials.
- Develop a plan to notify employees, management, and local authorities of a hazardous materials spill.
- Establish evacuation procedures.
- Consider creating and training an emergency response team.

If a spill occurs, follow the procedures created by your insurance agency as well as those mandated by regulation. Remember: Safety comes first!

FLOOD

Floods are one of the most frequent and costliest disasters for businesses. Some develop over a few days due to steady rain, and sometimes flash floods are caused by an intense storm, rapidly rising river, or dam failure.

To best prepare for a possible flood:

- Determine whether your facility is located in a flood plain.
- Review the history of flooding in your area.
- Review the community's flood response plan, especially evacuation routes and the location of higher ground.
- Establish warning procedures to notify employees.

- Inspect your facilities for the potential impact of flooding.
- Consider the need for flood-proofing (permanent or temporary).
- Identify equipment and records that should be moved to a higher location (such as putting computers on the second or third floors, on top of desks, or even removing them to dry storage facilities).
- Ask your insurance carrier about flood insurance and recommendations for flood protection measures.
- Unplug all equipment.
- Move vehicles to higher ground.
- Move any materials stored outside indoors.
- If your facility is on high ground and employees might need to take shelter in your facility during a flood, stock up on necessary supplies, such as water, nonperishable food (MREs), blankets and pillows, flashlights, batteries, and sanitation supplies.
- Establish an employee communication plan.

In the event that your business becomes flooded, there are certain actions you'll want to take. First and foremost, account for all employees and only return to your facility after officials have declared it safe.

Before doing that though, look for downed or damaged power lines, damaged gas lines, foundation cracks, collapsed roofs, or other external damage. Watch also for snakes and wild animals that might have entered your facility during the flood.

If you smell natural gas or hear hissing from a pipe, leave immediately and call the fire department. Also, wear protective clothing during cleanup, including gloves, boots, safety glasses, and respirators. Dispose of damaged materials safely and discard any perishable items that have come into contact with floodwaters.

If you have carpeting, pull it up and remove it. It also helps to run fans, air-conditioning, or heaters to encourage the drying process. For records that became wet, carefully separate one page at a time and lay them out individually. Finally, before turning the power back on, have an electrician evaluate all electrical systems.

HURRICANE

Hurricanes are a complicated combination of torrential rain, high winds, and storm surges that all may affect your operations differently. One good thing about them, though, is the amount of advance warning you get—usually 3 to 10 days—allowing you plenty of time to prepare. Some of the actions you can take to better protect your business against these extremely damaging storms include:

- Review the community's hurricane response plan, especially evacuation routes and the location of higher ground.
- Establish procedures for facility shutdown and early release of employees.
- Determine when you will let employees leave to prepare their homes.
- Establish an employee communication plan.
- Survey your facility and grounds and make plans to protect outside equipment.
- Bring inside anything that could be windblown, such as picnic tables and chairs.
- Trim tree limbs prior to hurricane season.
- Plan for window protection (storm shutters or thru-bolted exterior plywood).
- Evaluate whether the company needs a backup generator.
- Install and test battery-powered lighting.
- Stock up on flashlights and extra batteries.
- Prepare to move computer equipment and records away from windows, or to facilities on higher ground.
- Turn off propane and natural gas.
- Buy pumps so that buildings can be kept from flooding.
- Stock up on first aid supplies.
- If your facility is on high ground and employees might need to take shelter in your facility during a flood, stock up on necessary supplies, such as water, nonperishable food, blankets and pillows, flashlights, batteries, and sanitation supplies.

If a hurricane does hit, like with other disasters, the first thing you want to do is account for all employees and return to your facility only after officials have declared it safe. Stay out of any building that has water surrounding it, and if you smell natural gas or hear hissing from a pipe, leave immediately and call the fire department.

Wear protective clothing during cleanup, including gloves, boots, safety glasses, and respirators, and dispose of damaged materials safely. Discard perishable items that have come into contact with floodwaters, and pull up or remove carpeting that became wet, running fans to speed up the drying process.

For records that became wet, carefully separate one page at a time and lay them out individually to dry. And before turning the power back on, have an electrician evaluate all electrical systems.

EARTHQUAKE

An earthquake is a sudden and violent shaking of the ground, often striking without warning. They can occur at any time of year and any time of day, creating significant structural damage and disrupting utilities in the process.

Although these events are usually more common in certain parts of the United States than others, all 50 states have recorded them. Additionally, 45 states and territories are considered to be at a moderate or high risk.

What can you do to best prepare for a quake?

- Assess your facility's vulnerability to earthquakes, requesting seismic information from the local emergency management office.
- Contact your insurance agent regarding earthquake insurance; ask him or her for preparation recommendations.
- Have your facility inspected by a structural engineer.
- Inspect nonstructural systems, such as HVAC, water, and telecommunications for vulnerabilities.
- Inspect your facility for any items that could spill or fall during an earthquake.
- Install safety glass where appropriate.

- Secure heavy equipment and machinery to the floor.
- Secure piping.
- Store facility design drawing and blueprints off-site.
- Train employees on earthquake response and evacuation procedures.
- Conduct earthquake drills.
- Evaluate the location of critical documents, *consider that much earthquake damage is due to the triggering of fire sprinkler systems.*
- Review the community's earthquake response plan, especially evacuation routes and the location of higher ground (in case of flooding it is good to know the closest area of higher elevation).

If an earthquake hits, expect and prepare for aftershocks. Don't reenter your facility until it has been deemed safe by the appropriate authorities, and look for damage outside the facility.

If you smell natural gas or hear hissing from a pipe, leave immediately and call the fire department. Additionally, when starting cleanup, wear protective clothing, including gloves, boots, safety glasses, and respirators, and dispose of damaged materials safely.

TORNADO

Tornadoes are created by powerful thunderstorms and tend to strike with very little warning. Their high winds are capable of destroying solid structures and will turn ordinary objects into deadly missiles. One fairly recent tornado even picked up a lightweight pickup truck and deposited it five miles away.

Although they are most common in the Midwest and Southeast, like earthquakes, tornadoes have been reported in all 50 states. Therefore, to prepare your organization for this type of disaster, you want to:

- Ask your local emergency management office about the community's tornado warning system.
- Purchase a NOAA weather radio with a warning alarm and a battery backup.
- Establish procedures to notify employees of tornado warnings.

- Work with a structural engineer to design shelter areas in your facility.
- Consider the amount of space you'll need to shelter your employees and necessary supplies.
- Train employees on tornado response procedures (whether inside or outside of your facility).
- Conduct tornado drills.
- Trim tree limbs and remove dead trees.
- Secure outside equipment and furniture that could be picked up by the wind.

In the event a tornado forms in the vicinity of your business, exit your shelter only when officials deem it safe. Account for all employees and stay out of damaged buildings, watching for fallen or damaged power lines around you.

During cleanup, wear protective clothing like gloves, boots, and respirators. Dispose of damaged materials safely, and, if you smell natural gas or hear hissing from a pipe, leave immediately and call the fire department.

WINTER STORM

Winter storms bring cold temperatures, heavy snow, sleet, ice, and strong winds. Some even prevent employees from coming to work or customers from getting to your store. If severe enough, it may also close distribution channels or cause structural damage to your facility.

Some winter storms may affect only your community, whereas others stretch across several states. This makes preparation a must, not only for damage control but also for survival. During your preparations, here are a few things to consider:

- Establish procedures for facility shutdown and early release of employees.
- Establish employee communication procedures.
- For employees who cannot leave the facility, stock up on supplies, such as water, nonperishable food, blankets and pillows, and sanitation supplies.

- Stock up on flashlights and extra batteries.
- Consider acquiring a backup generator.
- Arrange for snow and ice removal from parking lots, walkways, and loading docks.
- Minimize or cancel employee travel.
- Winterize company vehicles.
- Contact your insurance agent for winter storm preparation recommendations.
- Have your heating system inspected and maintained prior to the start of winter.
- During severe low temperatures, consider running faucets to prevent pipes from freezing and bursting.
- Assist employees who may be stranded or have limited transportation.

HEAT WAVE

Heat waves and related droughts have caused more deaths than any other type of natural disaster. In some cases, high temperatures are accompanied by high humidity and put excessive strain on electric utilities. One of the top concerns during these types of events involves employees who are required to work outdoors. So, how do you best prepare?

- Pay attention to weather forecasts that involve temperatures in excess of 10 degrees above normal.
- Educate employees on safety precautions, including hydration, sun protection, and recognizing the symptoms of heat stroke and heat exhaustion.
- Provide employees with sufficient water and the appropriate protective clothing.
- Postpone noncritical outdoor work and activities during excessive heat times.
- Maintain equipment and vehicles for summer temperatures.
- Establish procedures to check on employees working outdoors by themselves.

FLU

Influenza, like a pandemic flu, such as H1N1, is a respiratory disease transmitted by a variety of viruses. It can strike quickly, easily spreading from employee to employee in the blink of an eye as the virus is transmitted by physical contact with germs. This usually occurs when a sick person sneezes or coughs into the air.

Flu season typically begins in the fall and continues through spring, although the flu may be contracted during any month of the year. To prevent this type of outbreak from paralyzing your business operations, take these prevention-based steps:

- Stay up-to-date on the latest flu types and outbreaks via the Centers for Disease Control (CDC).
- Consider paying for flu vaccines for your employees or providing a flu vaccination clinic onsite at your facility.
- Train employees on flu prevention methods, such as washing hands, covering their mouth when sneezing or coughing, and avoiding contact with others who are sick.
- Establish policies for sending people home when symptoms occur at work, extended sick leave allowances, and policies to allow employees to care for sick family members.
- Advise employees to stay home for at least 24 hours after a fever has gone.
- Stock up on disinfectant supplies and tissues.

Questions to Ask Yourself

1. Which special disasters are most concerning to my business?
2. What preventative measures can I take now to possibly keep them from occurring?
3. What measures can I put in place in case these disasters occur?

Conclusion

All businesses hope that they will never have the misfortune to suffer through a disaster. But, unfortunately, the odds are against us because at some point, every organization will likely experience some form of traumatic event. There really are only two kinds of companies: those that have experienced a disaster, and those that will experience a disaster.

Therefore, the best thing we can do for our organizations is to be prepared. Although avoiding disasters is the best we can hope for, the next best thing is to have an efficient and effective response if they do strike.

By following the actions in this book, your organization will be better prepared to not just survive a disaster situation, but to thrive during the process. Don’t be the type of company that says, “I wish I had taken the time to prepare.” Be the one that says, “I’m so glad we prioritized disaster preparation and response because this wasn’t nearly as bad as it could’ve been.” You’ll give your company and everyone associated with it a better chance of survival when you take a proactive approach.

APPENDIX A

Insurance Coverage Worksheet

	Type of Insurance	Agent or Broker	Contact Number	Email Address	Carrier	Policy Number	Policy Period	General Description	Exclusions or Limitations	Deductible	Waiting Period
General Liability											
Property Damage											
Business Interruption											
Dependent Properties											
Cyber											
Flood											
Automobile											
Product Liability											
Environmental											
Employment Practices											
Officers and Directors											
Errors and Ommissions											

APPENDIX B

Risk Analysis Worksheet

Column 1: List your threats. List all of the threats that have the potential to harm your business, but don't be concerned with putting them in any order yet. Leave out any threats that have a zero chance of occurring. For example, if you live in Oklahoma, there is a zero chance of being hit by a hurricane. Though some events may not seem likely, they should still be listed. For example, many people would not list an earthquake unless they had a facility in California, but earthquakes have occurred in all 50 states.

Column 2: Estimate probability. Indicate the likelihood of the threat occurring, with 1 being least likely and 5 being most probable. For example, if you live in southern Florida, you would rank a hurricane as a 5, or most probable. However, if you live on the New Jersey shore, you might rank a hurricane as a 2 or a 3.

Column 3: Assess the potential human impact. Evaluate the potential for death or injury. The lowest impact would be scored a 1 and the highest a 5. For example, the potential human impact of a tornado might be a 4 or 5.

Column 4: Assess the potential property impact. Evaluate the potential for damage to property. Consider impact to buildings, equipment, machinery, computers, inventory, and furniture and fixtures. When rating from 1 to 5, consider also the costs to clean or repair the items, the costs to set up a temporary replacement, and your costs (as well as your ability) to replace the damaged items.

Column 5: Assess the potential business impact. Evaluate the potential overall business impact of an event. Will you lose revenue, customers, or market share? When rating from 1 to 5, consider the length of business interruption; the extent of the business impacted (number of departments/functions); the ability of employees to come to work; customers' abilities to reach your business or place an order; interruption of manufacturing supplies; interruption of distribution methods; potential breach of contracts; potential for penalties, fines, or legal actions; and potential for reputational damage.

Column 6: Assess the potential infrastructure impact. Rate the potential for the loss of infrastructure supporting your business from 1 to 5. Consider the impact of the loss of telephone systems, Internet, power (electric or natural gas), water supply, and roads and bridges.

Column 7: Evaluate the availability of internal resources. Assess the availability and quality of your internal resources to respond to an event. When rating from 1 to 5, consider the availability of cash, training of personnel, availability of equipment, and ability to quickly respond.

Column 8: Evaluate the availability of external resources. Assess the availability and quality of your external resources to respond to an event. When rating from 1 to 5, consider mutual aid agreements; availability of alternate suppliers; availability of alternate distribution methods; and availability of local, state, or federal emergency response.

Column 9: Estimate the restoration time. For each event, consider the length of time it will take you to restore your operations to normal. A rating of 1 may mean minutes and a rating of 5 may be months or years. For example, if your business is a bank, a power outage may be ranked a 1 in restoration time if you have a generator and have tested its ability to bring power back to normal.

Column 10: Total. After completing your assessments, add the scores for each event and enter a total in Column 10. The lower the score, the better. Then sort the list so that the highest-scoring events are listed first.

Threat	P	HI	PI	BI	II	IR	ER	RT	Total Score

P = Probability, HI = Human Impact, PI = Property Impact, BI = Business Impact, II = Infrastructure Impact, IR = Internal Resources, ER = External Resources, RT = Restoration Time

APPENDIX C

Damage Assessment Form

Category	**Condition**	**Priority**
Equipment		
IT equipment		
Communications		
Furniture		
Inventory		
Supplies		
Other		

APPENDIX D

Summary of Communication Systems

Type of Service

___ Telephone
___ PBX system
___ Internet provider
___ Mobile phone
___ Other

Description of Service

Provider Information

Company name: ______________________________
Phone number: ______________________________
After-hours number: ______________________________
Company representative: ______________________________

Recovery Procedures

APPENDIX E

Emergency Communications Summary

Roles and Responsibilities

Primary communicator: ______________________________
Contact information: ______________________________
____
____

Backup communicator ______________________________
Contact information: ______________________________
____
____

Stakeholders

___ Employees
___ Investors
___ Regulatory Agencies
___ Management
___ Customers
___ Media Outlets
___ Directors
___ Vendors

When to Activate Communications

Length of time of the outage or disaster: ________________
Severity of the disaster: ______________________________
Percentage or number of employees or departments impacted: ______________________________
Other: ______________________________________
____
____

Emergency Communications Plan

Attach the appropriate documentation for:

- Phone tree
- Evacuation plan
- Emergency notification system
- Voicemail or Internet updates

Message Templates

Attach copies of free prepared and approved messages for all stakeholders.

APPENDIX F

Business Continuity Plan Outline

1. Executive Summary
2. Introduction
    a. How to use the plan
    b. Objectives
    c. Scope
    d. Assumptions
    e. Plan maintenance
    f. Testing procedures
    g. Training procedures
    h. Plan distribution
3. Business Continuity Strategy
    a. Business function recovery priorities
    b. Relocation strategy
    c. Recovery plan phases
    d. Disaster occurrence
    e. Plan activation
    f. Alternate site operations
    g. Critical records
    h. Restoration of hardcopy files, forms, and supplies
    i. Access to computer systems
4. Disaster Response Team
    a. Objective
    b. Response team assignments
    c. Response team responsibilities
    d. Response team contacts
    e. Business continuity coordinator
    f. Communications
    g. Human resources
    h. Emergency response
    i. IT recovery

5. Disaster Response
    a. Purpose
    b. Response phases
    c. Prevention
    d. Disaster occurrence
    e. Plan activation, alerts, and warnings
    f. Facility shutdown
    g. Evacuation
    h. Shelter in place plan
    i. Assessment and mitigation
    j. Alternate site operations
    k. Communications
    l. Restoring functions
    m. IT recovery
    n. Transition to normal operations
    o. Specific events
    p. Earthquake, tornado, flood, hurricane, medical emergency, etc.
6. Supporting Documents
    a. Employee contact list
    b. Emergency contacts, including fire, police, hospital, emergency management, electrician, plumber, insurance agent, banker
    c. Recovery priorities
    d. Insurance summary
    e. Financial contacts
    f. Critical vendors
    g. Key customers
    h. Disaster response supplies
    i. Notification scripts
    j. Training and testing schedule

APPENDIX G

Schedule of Training and Testing

	Jan	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sept**	**Oct**	**Nov**	**Dec**
Management training												
Employee training												
Management exercise												
Response team exercise												
Walk-through drill												
Evacuation drill												
Full-scale exercise												

APPENDIX H

List of U.S. Privacy Laws

Americans with Disabilities Act (ADA)—www.eeoc.gov/laws/statutes/ada.cfm

Cable Communications Policy Act of 1984 (Cable Act)—www.law.cornell.edu/uscode/text/47/551

Children's Internet Protection Act of 2001 (CIPA)—www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/cipa/cipatext.pdf

Children's Online Privacy Protection Act of 1998 (COPPA)—www.law.cornell.edu/topn/childrens_online_privacy_protection_act_of_1998

Communications Assistance for Law Enforcement Act of 1994 (CALEA)—www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act

Computer Fraud and Abuse Act of 1986 (CFAA)—www.law.cornell.edu/uscode/text/18/1030

Computer Security Act of 1987—http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt

Consumer Credit Reporting Reform Act of 1996 (CCRRA)—http://epic.org/privacy/fcra/

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003—www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business

Driver's Privacy Protection Act of 1994—http://epic.org/privacy/drivers/

Electronic Communications Privacy Act of 1986 (ECPA)—www.law.cornell.edu/uscode/text/18

Electronic Fund Transfer Act (EFTA) Summary—www.fdic.gov/regulations/laws/rules/6500–1350.html

Fair and Accurate Credit Transactions Act (FACTA) of 2003—www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf

Fair Credit Reporting Act—www.consumer.ftc.gov/sites/default/files/articles/pdf/ pdf-0111-fair-credit-reporting-act.pdf

Family Education Rights and Privacy Act of 1974—www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Federal Information Security Management Act (FISMA)—http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Federal Trade Commission Act (FTCA)—www.ftc.gov/about-ftc/what-we-do/enforcement-authority

Gramm-Leach-Bliley Act (GLBA), also known as Financial Services Modernization Act of 1999—http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

Privacy Act of 1974—www.justice.gov/opcl/privacyact1974.htm

Right to Financial Privacy Act of 1978 (RFPA)—www.fdic.gov/regulations/laws/rules/6500–2550.html

Telecommunications Act of 1996—http://transition.fcc.gov/telecom.html

Telephone Consumer Protection Act of 1991 (TCPA)—www.fcc.gov/guides/unwanted-telephone-marketing-calls

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)—http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162

Video Privacy Protection Act of 1988—http://epic.org/privacy/vppa/

APPENDIX I

IT Backup and Testing Log

Type of information: ____

____

____

Type of media:

___Network ___Hard Drive ___ External Hard Drive/Flash Drive

___Laptop ___Cloud

Is it backed up? ___Yes ___No

Frequency of backup:

___Hourly ___Daily ___Weekly ___Monthly ___Quarterly

___Yearly ___Never

Location of backup: ____

____

____

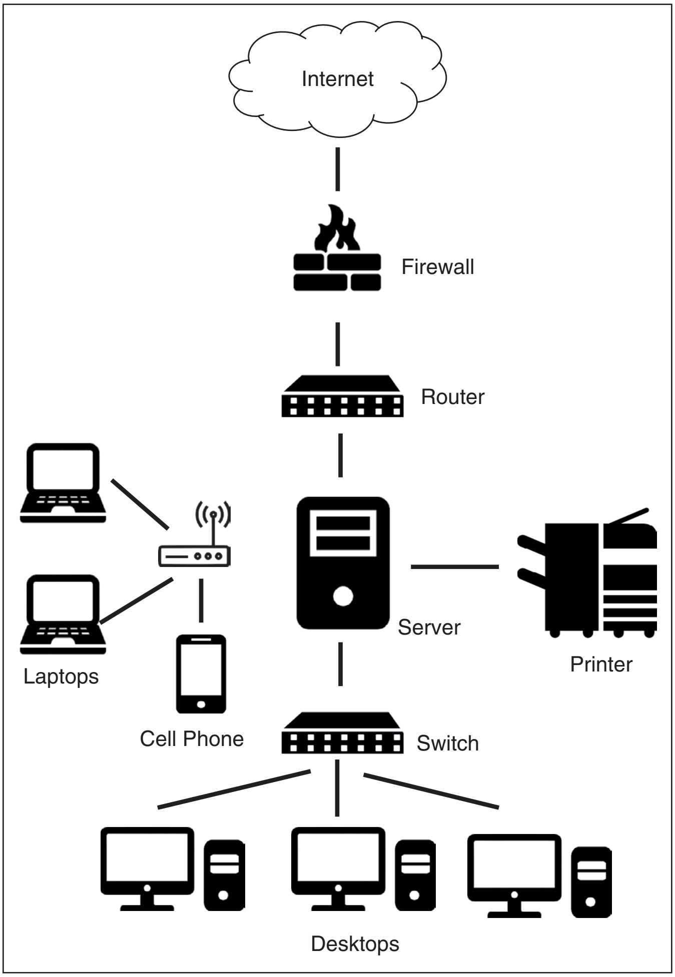
Date of last recovery test: ___________________________________

____

____

APPENDIX J

Sample Computer Network Map


Internet
Firewall
Router
Laptops
Cell Phone
Server
Printer
Switch
Desktops

About the Authors

Jennifer H. Elder is a Certified Speaking Professional (CSP), Certified Public Accountant (CPA), Chartered Global Management Accountant (CGMA), Certified in Financial Forensics (CFF), Certified Management Accountant (CMA), and Certified Internal Auditor (CIA). She works with finance professionals and organizations that want to ensure sustainable success by planning for the best and preparing for the worst.

As a consultant and keynote speaker, Jennifer is known for being energetic and enthusiastic. She has a natural talent for taking complicated topics and making them simple, practical, and immediately implementable. She has worked with the Fortune 500, US government, state CPA societies, and CPA firms in 48 states and 5 countries.

CPA Practice Advisor named Jennifer one of the "Top 25 Women in Accounting" in 2018. The AICPA and MACPA named her a "Woman to Watch" in 2015. She has been awarded Outstanding Educator by the AICPA five times.

In 2018, Jennifer earned the designation of Certified Speaking Professional (CSP). She is 1 of only 10 people worldwide who hold both the CPA and CSP designations.

Her experiences with disasters include "Snowmaggedon" when Washington, DC, received 77 inches of snow and was closed for over a week; a rare earthquake in Richmond, Virginia; a power outage from an ice storm in New Hampshire; industrial sabotage days before the sale of a business; a lightning strike that disabled a phone system and entire customer service department; and surviving 4 hurricanes in 13 weeks working for a home builder in Florida where more than 200 homes under construction were damaged multiple times.

Samuel F. Elder is a retired ship's captain who has worked and lived in over 54 countries. Operating ships, Captain Elder regularly encountered combinations of hurricane force winds, rogue waves, massive currents, excessive tides, and shipboard fires.

At sea, preparing for the worst is mandatory; the only resources you have to draw on are what you brought with you. The industrial working loads involved in running a ship, loading heavy cargo, and coping with the weather are so massive that merchant sailors must live in a world where training, situational awareness, and common sense are the only things separating them, their crew, and their passengers from life and death.

Index

WILEY END USER LICENSE AGREEMENT