BRACING FOR IMPACT

A PRACTICAL GUIDE TO PREPARING FOR DISASTERS

PAUL T. MARTIN

Bracing for Impact

A Practical Guide to Preparing for Disasters

Bracing for Impact

A Practical Guide to Preparing for Disasters

Paul T. Martin

Austin 2011

The State Bar of Texas, through its TexasBarBooks Department, publishes practice books prepared and edited by knowledgeable authors to give practicing lawyers as much assistance as possible. The competence of the authors ensures outstanding professional products, but, of course, neither the State Bar of Texas, the editors, nor the authors make either express or implied warranties in regard to their use. Each lawyer must depend on his or her own knowledge of the law and expertise in the use or modification of these materials.

The opinions expressed in this book do not necessarily represent the views of State Farm Mutual Automobile Insurance Company or any other State Farm affiliate. Readers are encouraged to seek professional guidance from a qualified source for instructions on how to implement incident response or business continuity plans to meet each reader's unique situation.

International Standard Book Number: 978-1-892542-80-9
Library of Congress Control Number: 2011931982

Austin, TX 78711

Printed in the United States of America

For Kendel and Delaney:

Many of my colleagues encounter my fascination with this topic
from time to time. You patiently endure it daily,
even when it seems strange.
And for that, I love you very much.

Paul T. Martin

Paul T. Martin graduated from Vanderbilt University in 1992 with a bachelor of science in public policy studies. He earned his juris doctor from the University of Miami in 1995.

Licensed in Tennessee, Florida, and Texas, Paul has actively practiced law in those states during his career as an insurance defense attorney in private practice and as in-house counsel for State Farm Mutual Automobile Insurance Company.

In addition to his legal duties at State Farm, he regularly consults and trains its employees on incident response and business continuity matters. He is also assigned to State Farm's Crisis Management team for its operations in Texas.

Paul is a former volunteer firefighter, a licensed ham radio operator, an instrument rated pilot, an NRA-certified firearms instructor, and a trained storm spotter for the National Weather Service.

STATE BAR OF TEXAS

BOB BLACK
PRESIDENT

Direct Correspondence to:
2615 CALDER, STE. 800
BEAUMONT, TX 77704
TEL: (409) 835-5011
FAX: (409) 835-5729
bobblack@mehaffyweber.com

The State Bar of Texas is proud to publish *Bracing for Impact: A Practical Guide to Preparing for Disasters*. For more than five decades, the State Bar has published books that offer Texas lawyers important resources to improve their practices. This useful desk reference continues that tradition by highlighting various disasters that might impact law offices and identifying methods through which attorneys can prepare for them.

The State Bar wishes to acknowledge its deep gratitude to author Paul Martin for sharing his knowledge and guidance on this important subject. His dedication to ensuring that law offices have the ability to function efficiently during crises and desire to support fellow attorneys made this work possible.

Bob Black
President, State Bar of Texas

Contents

Preface

"Don't eat the whole box of chocolates," I admonish my eight-year-old son, "or you'll make yourself sick." As the words echo in the dining room, I add silently to myself, *"Don't ask me how I know that."* My son asks to be excused from the table, clearly rejecting my fatherly wisdom. I recall this elemental story every time I learn something new—which is quite often—from someone whose life experience and expertise command my attention.

This brings me to Paul Martin's book. When Paul Martin and I first talked about *Bracing for Impact*, I had already been aware of the project for some time. My friends at the State Bar knew I'd be interested in the book. After all, my offices in downtown Fort Worth, located on the thirty-fourth floor of the Bank One Tower, were demolished by a tornado in March of 2000.

As a result of that tornado, the Bank One Tower was one of eight buildings ultimately condemned in the downtown area, along with twenty-seven others that sustained major damage. My coworkers and I went from preparing for a major jury trial that was to take place the following week to wondering how many employees would need to be laid off because the civil disaster authorities would not let us in the building to retrieve our computers, our files, our lives. We were the fortunate ones, though. The same tornado killed two people and injured eighty others that day.

In the pages that follow, readers will learn that there are accidents that cause financial injury on the one hand, and tragedies resulting in the loss of life on the other. Because these life-changing events are, to some extent, foreseeable, we must be diligent in every respect to minimize both outcomes. With Paul's capable assistance, *Bracing for Impact* can help us do that.

This book will help you think about the unthinkable. It lays the groundwork for a successful recovery strategy. It discusses available insurance coverages and common sense supplies to have on hand in case they are needed. It describes readily available technologies for our computer systems and procedures for delegating specific tasks to staff members in case of emergency. It is one-stop shopping for "Disaster 101."

Take these valuable suggestions to heart. Collaborate with your coworkers or hire professionals to assist you in implementing the protocols recommended; if you're a solo practitioner, make a checklist of what you can do to protect your family from a recoverable event. Thanks to Paul's excellent work, you don't need to invent a strategy yourself. The template is within these pages. All you must add is individual effort. I personally urge you, in the strongest terms, to expend that effort. You won't regret it.

Don't ask me how I know that.

Tim Chovanec
Attorney at Law
Fort Worth, TX

Acknowledgments

Having never written a book before, I quickly learned that such a project is indeed a group effort. A number of people helped shape the message, and I am forever grateful to them.

Several fantastic women at the State Bar of Texas—Sharon Sandle, Vickie Tatum, Ellen Pitluk, Courtney Cavaliere, and Diane Morrison—made this book a reality. Likewise, former State Bar employee Ann Kloeckner greatly assisted in the creation of this book. Despite the fact that this subject matter deviates from what one might expect from a state bar association, these ladies gave me the creative license to try something new. For that opportunity, I am very grateful.

Many colleagues at State Farm Insurance have, over the years, influenced the content of this book. Scott Cox, David Nix, Julie Jansen, Richard Page, John Stuckemeyer, and Tom Doluisio have helped me refine the message by prodding me to think about the various challenges business owners face during and after a disaster. Their willingness to engage me on a number of topics and to review portions of the manuscript was quite helpful in the writing process.

My sister-in-law, Kristin Bailey, PhD, had the unenviable task of serving as first draft editor. She generously agreed to review and edit my work as a Christmas present to me, and her touch is firmly embedded throughout this book.

A number of lawyers—James Keim, Jeff Kilgore, Dan Steppick, and Jeff Tormey—helped in one way or another with their feedback and stories of disasters affecting lawyers. I cannot tell you how wonderful it is to reach out to fellow lawyers for assistance and to receive far more than you ever expected.

Bracing for Impact

A Practical Guide to Preparing for Disasters

Introduction

I volunteered to write this book in part to better understand my own fascination with disaster preparedness. My interest in the subject began at the ripe old age of five. During an unseasonably warm afternoon on March 12, 1975, a major storm system blew through Shelbyville, Tennessee, resulting in dramatic damage to a number of homes, schools, and businesses.

I remember the day well. I had just returned from my part-time daycare and was having lunch with my friend Casey and one-year-old brother Jerry. Out of the blue, my mother scooped Jerry out of his high chair and ordered Casey and me to run into the hall and lie down on the floor. The wind howled; we had to yell in order to hear one another. My mom went back into the kitchen and retrieved our lunches, which we ate, quite calmly, while lying on the floor of our home on Perfection Drive.

I quickly found out, however, why my mother had gone into crisis mode. While we had been sitting in the kitchen, she had watched our next-door neighbor's front porch blow off of his house and into our backyard. After the storm, we went outside to examine the aftermath. Debris littered the entire neighborhood, including trash cans, lawn furniture, large chunks of tool sheds, roofing shingles, and, of course, our neighbor's front porch.

My mom and I spent the afternoon helping our neighbor secure his belongings, and we later learned that another neighbor had been admitted to the local hospital due to the storm. It was a very exciting experience for a five-year-old Tennessee boy who had always been fascinated with weather and disasters on the evening news.

As I got older, my fascination with disasters (and preparing for them) didn't wane. As a grade-school student, I listened to discussions about the Iranian hostage crisis, rising tensions in the Middle East, and why Charlie Daniels's song "In America" should become our de facto national anthem. In junior high and in high school, I read books and watched movies regarding how the Soviets planned to attack the United States. And on beginning law school, my life was impacted by yet another disastrous storm.

I moved into a studio apartment in South Miami in 1992 to begin my law school experience at the University of Miami. While unpacking and preparing to begin classes, local news stations informed viewers that the then-category 5 Hurricane Andrew would be hitting Miami in thirty-six hours. "Great," I thought. "I hardly know a soul in Miami, my car is in the shop for radiator work, and I have no idea what I am supposed to do to prepare for a hurricane."

Fortunately for me, I found a way to ride out the storm by evacuating to Orlando. *Unfortunately* for me and for many others, the storm severely damaged my apartment, the law school, and the homes of several professors and fellow students. I felt rather inadequate, to say the least. I had no disaster supplies, other than an oil lantern my mother had sent with me "in case of a power outage" and a small battery-powered radio.

I returned to my apartment shortly after the storm. For seventeen days, I endured the misery of living in Miami in the summer heat without electricity. I ate Spam fried on a gas stove. To this day, I can't stomach the thought of eating it ever again. I drank water that I first had to boil, complying with the "boil water" order issued by local authorities. In an effort to keep us on schedule despite the three-week delay in our class start date, professors gave us reading assignments. At night, I read torts by oil lamplight (imagining how Abraham Lincoln must have felt doing the same).

School eventually resumed, and Miami eventually recovered. I overheard stories of how some students left Miami before school even started, having lost so much from the storm. Professors lived in alternative housing for months while their homes were repaired.

I was a bit better prepared for the Y2K nonevent. Having had some lead time, I stocked up on food and "preparedness toys" (discussed in detail in chapter 10). More importantly for me, I began to reflect more on the importance of disaster preparedness and my own strong interest in the topic.

Just twenty months later, citizens across the United States would feel the effects of a truly terrible disaster—terrorism. At the time of the 9/11 attacks, I was working in a litigation practice in Fort Lauderdale. For days after the attack, the court system closed down completely—there were no hearings, trials, or judicial conferences. Every package left unattended received an unimaginable level of scrutiny. And God help you if you looked "suspicious" while walking around the courthouse.

Our cable news outlets now show European rioting in real time—riots spurred by austerity measures enacted by various European governments. In our own hemisphere, violence along the Mexican border remains at depressingly high levels, hurricanes hit populated areas, tornadoes hit high-rise office buildings, water pipes burst and flood businesses, buildings catch on fire, law firm employees become domestic violence victims, fans of champion NBA teams riot in celebration, and on and on. Disasters of all sizes, shapes, and flavors have occurred throughout history and will be with us for all of our days.

Think about that for a moment—you *know* these events will happen sometime, somewhere. Does it make sense to prepare your firm for that possibility? Our law firms and legal departments are some of our biggest assets. Preserving these valuable assets in the face of danger helps us in our personal and financial lives, which in turn enables us to help our clients. It is my hope that you will learn something from this book that will better enable you to protect your firms and departments from the dangers described above.

Use what you can from this book. Discard the rest. Create a plan. Implement it. Regularly update and exercise it. And sleep better at night as a result.

Chapter 1

Disasters and Law Offices

Jeff Kilgore knew.

Elected president of the Galveston County Bar Association the summer of 2008, Kilgore and other bar leaders planned a continuing legal education (CLE) presentation on disaster preparedness for law firms for late September of that year. The events of September 13, however, changed those plans dramatically.

Hurricane Ike made landfall in Galveston in the early hours of September 13, bringing category 2 strength winds along with a category 4 storm surge. The storm continued inland into Houston, causing a tremendous amount of damage. In addition to the destruction of homes, businesses, and infrastructure, many people in Texas, Louisiana, and Arkansas died as a result of Ike's wrath.

Kilgore knew something like this could happen. He had made some basic plans to protect his mediation practice from severe weather, including maintaining an office on the second floor of a brick building with small windows. As the storm approached, he backed up his

computer files using an external hard drive, then went home to prepare his house and family for the coming storm. But after the storm, Kilgore discovered that the water damage to his office had been far worse than he had anticipated. Wind-driven rain damaged paper files, including papers locked securely in his desk.

"Rainwater and debris trashed the whole office," he later told me.[1] "When I opened a drawer in my desk with personal papers like my marriage license and my scuba diving log books, it was filled with water, turning everything in the drawer into papier mâché."

During his tenure as bar president, which turned out to be one of the most critical times for the profession in Galveston County, Kilgore estimates that over one hundred law offices were displaced. Most of these unfortunates were solo practitioners or very small partnerships. In many instances, it took nine months for lawyers to establish alternative office space.

Many of these firms rented their office spaces and did not have renter's insurance to cover damage to their furniture or computers. Kilgore reports that the larger firms fared better if they had multiple offices to which they could move their Galveston operations after the storm.

While the loss of office space and furnishings was a big problem for Galveston lawyers, an even bigger one turned out to be communication with clients. The Galveston County Bar took out full-page ads in the local newspapers to tell clients how to get in touch with their attorneys after the storm. Many attorneys lost all contact with some clients, never to be reestablished.

As many of us have come to expect, those lawyers who were able to help colleagues did so. These practitioners shared office space, computers, and other resources to help their colleagues get back on their feet. In addition, the Galveston County Bar worked tirelessly to help get the court system and lawyers back on track. Kilgore added that "the district and county clerk offices did a great job in keeping things going" after the storm.

---

1. Jeff Kilgore, e-mail message to author, December 21, 2010.

In reflecting on what he might have done differently to better prepare for the storm, Kilgore's advice for other lawyers is short and succinct:

- Take the computers with you. Backing them up is important, but computers are small enough that it doesn't take much to pack them, along with the peripherals. Having access to your computer files and to the Internet can help you get your practice back on track quickly.
- Scan. Keep files and even evidence in a digital format, if possible.
- Find an easy, reliable way to do computer backups. Kilgore prefers using external hard drives over online backup systems, such as "cloud computing" (discussed in chapter 4).
- Keep the CDs for operating system software. Many people throw these CDs away after installing software or don't opt to pay the few extra dollars to get the CDs if they download the software from the Internet. Having these available can make computer restoration much quicker.
- Make sure you have adequate insurance to cover your office furniture and equipment, as well as lost income. Even attorneys who rent space should make sure their insurance is adequate to protect them from disasters.
- Keep in mind that various types of disasters may affect an office. Tornadoes, fires, wind, loss of power, and power surges all need to be considered when establishing a plan to keep your office and your clients' records safe. Storage of current files is one of the biggest challenges. Our court systems are going to digital records and filing, and so should we.

The situation that occurred in Galveston is not uncommon. Businesses of all types and sizes suffer from the effects of disasters. Storms, fires, plumbing failures, and even workplace violence can hamper a business's ability to continue and take a toll on its employees.

The good news is this: while we can't always avoid disasters, we can take steps to prepare for them. These steps need not be time-consuming or costly. In the coming pages, we will study the need to prepare, the risks we face, and the steps we can take to avoid the effects of a catastrophe in our offices.

Chapter 2

Why We Don't Prepare for Disasters

Back in high school, I had a history teacher who always delivered pithy sayings about history, education, and life in general. When we would complain about studying for one of his tests or working on a project, he would smile and simply say, "Those who sweat in practice don't bleed in battle."

In this age of twenty-four-hour news cycles, it is not hard to find people who failed to heed this advice. Intense storms and hurricanes, wildfires, earthquakes, shootings in the workplace, and other random violence permeate news programming. While disasters cannot always be averted, we *do* know they are going to happen. After a major disaster like Hurricane Katrina, you might assume that people would learn from prior mistakes and make better efforts to prepare for such events.

And yet we don't. In 2006, roughly one year after Hurricane Katrina devastated the Gulf Coast, *TIME* magazine ran an article entitled, "Floods, Tornadoes, Hurricanes, Wildfires, Earthquakes . . . Why We Don't Prepare." *TIME* concluded:

> In fact, 91% of Americans live in places at a moderate-to-high risk of earthquakes, volcanoes, tornadoes, wildfires, hurricanes, flooding, high-wind damage or terrorism, according to an estimate calculated for TIME by the Hazards and Vulnerability Research Institute at the University of South Carolina. But Americans have a tendency to be die-hard optimists, literally. It is part of what makes the country great—and vincible.
>
> "There are four stages of denial," says Eric Holdeman, director of emergency management for Seattle's King County, which faces a significant earthquake threat. "One is, it won't happen. Two is, if it does happen, it won't happen to me. Three: if it does happen to me, it won't be that bad. And four: if it happens to me and it's bad, there's nothing I can do to stop it anyway."[1]

If you are reading this book, it's because you are interested in preparing your law firm for a potential disaster, be it man-made or otherwise. However, you may have people within your organization who are not as concerned about the need to make such preparations. It's imperative that we understand the mindset behind those who don't think preparing for disasters is important. In doing so, we can create approaches to convince them otherwise.

I've identified four basic objections to why a firm (or any business for that matter) should implement a disaster plan. These include:

1. *The cost of implementing and testing an incident response or business continuity plan is too high.* Generally, this response comes from small firms who think such plans are only for large, well-capitalized organizations. Fortunately, more and more firms are realizing that incident response and business continuity planning need not be costly. In fact, many smaller firms are able to create such plans for a tiny fraction of what larger firms are spending for the same thing.
2. *I really don't care if I have a disaster plan or not; it's just not that important.* Apathy kills. It kills businesses

1. Amanda Ripley, "Floods, Tornadoes, Hurricanes, Wildfires, Earthquakes . . . Why We Don't Prepare," *TIME Magazine*, August 28, 2006, 54.

and law firms. This kind of response is more likely to come from an employee than from an owner of the business. It may also come from someone who does not appreciate the potential risks the business faces.

3. *Maybe if we don't talk about it, it won't happen.* I call this "denial caused by fear." For those of us who believe in preparedness, this is perhaps the hardest mindset to understand. The person genuinely appreciates the prospect of a disaster but wants to avoid worrying about it by not planning for it.

4. *Even if something bad does happen, my business won't be affected by it.* I refer to this as "denial caused by naïveté." Many entrepreneurs and business owners are eternal optimists and risk takers. They've gotten this far by not having a plan for disasters; why have one now?

In your efforts to get other members of your organization on board, here are some strategies you might follow:

- Ask, "Why don't you think we need to prepare?" Sales people are trained to ask lots of probing, open-ended questions to identify the buyer's objections to the sale. In essence, you are trying to "sell" the need to prepare. By asking open-ended questions such as this one, you will have more success in determining where the objections lie and how to address them.

- Share examples of other law firms' and businesses' misfortunes as a result of disasters. For many people, workplace violence is something that happens to "other people." When we hear about it happening at a law firm our size, with the same practice area that our firm has, the story hits much closer to home. Share those news reports with your colleagues, and ask, "What would we do in that situation?"

- Involve your insurance agent. Insurance agents and claim adjustors are in the business of mopping up disasters. Day in and day out, they hear stories of everything from burst pipes causing extensive damage to a business's computer system, to electrical fires rendering an office space uninhabitable, to complete

and total loss of a business due to a weather event. Insurance agents love to tell stories to clients in order to sell insurance products. In-depth discussion of the types of insurance a firm might need is provided in chapter 9.

- Be persistent. Several years ago, I began doing some basic incident response and business continuity planning for my legal department. While these actions were well-supported by my supervisor and by some of my colleagues, other shareholders in the organization wondered why I was so "paranoid." However, as time went on, with the advent of things like pandemics, massive hurricanes, and terrorism, many of those people who thought I was being paranoid came to see the value in having a good plan in place.

As we saw in chapter 1, disasters can befall attorneys and their legal practices. While we cannot always prevent disasters, we can "sweat in practice" and minimize the impact such events might have on our law offices. Taking the steps now, which need not be time-consuming or expensive, can yield tremendous benefits in the moments after a disaster.

Chapter 3

The Threats We Face

On the sunny morning of February 18, 2010, a disturbed individual with a tremendous amount of anger at the Internal Revenue Service flew his airplane into one of its Austin branch offices. Less than an hour after the incident, I drove by the crash site on Highway 183 on my way to a lunch meeting. As traffic crept past the site and motorists gazed at the gaping hole in the side of the Echelon building, I listened to a local talk radio show. People were calling in, sharing their opinions about what had happened. One person commented that he would never have imagined that someone might fly a plane into the side of his building.

Why would anyone think something like this could happen in Austin? Because it can happen anywhere. The Austin plane crash, the Oklahoma City bombing, and the Atlanta Olympic Park bombing are but a few examples of terrorist acts occurring outside New York or Washington. To prepare ourselves, we have to face reality: bad things can happen to us, and they can happen at *any place.* If I were to ask you what possible disasters might affect your office, I suspect you

could give me a good list of relatively common ones in short order. However, the purpose of this book is to help you prepare for every *conceivable* disaster. That means that we have to start thinking of rarer, less predictable disasters, in addition to those that seem more commonplace.

For the purpose of this discussion, I'm dividing the threats that attorneys face into three distinct groups: *natural disasters, man-made disasters,* and *intentional acts*.

Natural Disasters

In researching ideas about the possible natural disasters that might impact a legal office, one need only turn on a cable news station and watch for a few minutes. Invariably, news outlets run stories on various natural threats affecting people, homes, and businesses.

In my opinion, that same media often create more hype and harm than is necessary to address a particular risk. Wall-to-wall coverage of severe thunderstorms, wildfires, and the dreaded pandemic seems to imply that these perils will affect almost every American in a catastrophic way. In reality, these things, while serious, should be taken in context. The vast majority of Americans will not have their homes swept away by raging floods or F5 tornadoes. Most Americans won't die of a pandemic disease or lose their homes to an out-of-control wildfire.

It's my hope to give you some things to think about in terms of what natural disasters might affect your business. Accordingly, let's look at the following possibilities.

Weather

Disastrous weather events often include severe thunderstorms, tornadoes, and hurricanes. These three events may bring large hail, damaging winds, and torrential rain. As you can imagine, an office suffering wind, hail, or water damage could easily be out of commission for an extended period of time. What specific issues might arise from these events?

- *The inability to use the office*. If the office is uninhabitable, you will need to find an alternative work site on a temporary basis or perhaps even on a permanent one.
- *Damage to computers, furniture, and files*. If you cannot access your computer or your paper files, you'll likely find practicing law quite difficult. In addition, at some point you're going to want to sit down at a desk or table to get some work done. If those items are inaccessible or damaged due to the weather, they will need to be replaced either on a temporary or permanent basis.
- *Lack of utilities*. In a less severe situation, your building will remain intact, but there's a chance you will not have power, Internet access, and/or water. Not having these key utilities could also render your law office helpless.

Wildfires

Let's make two quick points about wildfires. First, as humans encroach upon wilderness areas, the risk of wildfires increases. Second, wildfires are not limited to California. Texas has experienced a number of wildfires over the past few years, particularly in northwestern counties.[1, 2] Drought conditions brought on by long-term weather phenomena exacerbate the risk.

Whereas a single building fire damages one building and the businesses located within it, wildfires are capable of destroying large portions of an urban or suburban area. Further, they make those areas impassable to people who need to pass through them to get to their offices.

1. Office of the Governor Rick Perry, "Texas Continues to Battle Panhandle Wildfires," news release, March 14, 2006, **http://governor.state.tx.us/news/press-release/2469/**.

2. Office of the Governor Rick Perry, "Gov. Perry Again Renews State Disaster Proclamation Due to Ongoing Wildfire Threat," news release, May 13, 2011, **http://governor.state.tx.us/news/press-release/16129/**.

Earthquakes

Even in Texas we get earthquakes from time to time. While they are small and tend to be concentrated in the Panhandle, the entire state has some level of earthquake risk.

According to the Texas Department of Public Safety, within the twentieth century Texas experienced more than one hundred earthquakes large enough to be felt. Their epicenters occurred in forty of Texas's 254 counties. Four of these earthquakes had magnitudes between five and six, which means that they were large enough to be felt over a wide area and cause significant damage near their epicenters.[3] Like severe weather aboveground, earthquakes can render an office and its contents inaccessible. Further, dangers from broken gas mains, and from unsafe infrastructure such as buildings and bridges, compound the problem.

Pandemics

Reports of the H5N1 and H1N1 flu outbreaks caused a fair amount of consternation among disaster planners. It's important to remember, however, that pandemics have been recorded throughout history. Three pandemics of influenza occurred during the twentieth century, and, as of the date of this publication, there has been one flu pandemic during the twenty-first century.[4]

Simply put, a pandemic is an epidemic over a wide geographical area. In a pandemic, technology cuts both ways. While medical technology allows us to respond with more sophisticated treatment and prevention, other useful devices of technology, such as worldwide shipping and international flights, can spread the disease worldwide in very short order. Pandemics present unique challenges to disaster planners. Some of these challenges include:

---

3. "The State of Texas Mitigation Plan," last modified October 25, 2007, accessed May 18, 2011, **www.tcrfc.org/docs/tx_mitigation_plan_2007.pdf**.

4. "Flu Pandemics," Flu.gov, accessed May 18, 2011, **www.flu.gov/individualfamily/about/pandemic/index.html**.

- People may not want to work or interact with others.
- People may be reluctant to travel.
- The workplace may contain pathogens on various surfaces, such as doorknobs, furniture, and electronic equipment.
- Critical infrastructure, such as utilities or delivery of gasoline and groceries, may be massively impacted.
- Unlike a severe weather event or other natural disaster, the fear of the threat—getting infected—may last for weeks or longer.

Man-Made Disasters

Mother Nature's wrath provides plenty of incentive to be prepared for disasters. But let's not forget disasters due to accidents or breakdowns in our man-made infrastructure, such as the following.

Chemical Spills

Every day, tractor-trailer trucks, container ships, barges, and railroad cars carry all sorts of substances hazardous to our health. While these substances are arguably necessary for a modern-day economy, they can cause serious injury and death if not handled properly.

Many people don't realize their susceptibility to chemical spills. If your office is located near a major highway, waterway, or railroad track, your risk of a chemical spill issue grows dramatically.

In addition to the risk of chemicals in transport, don't forget about the neighbors in your office building or office park. In Austin, where I live, we have a number of high-tech companies that regularly use dangerous substances in the making of computers and technical devices. Oftentimes, these businesses have rented space in large office complexes, next to other businesses that may be completely unaware that those dangerous substances are nearby.

Office Fires

An office fire can have devastating effects on a business. As with any disaster, tangible assets as well as intangible ones can be lost.

As a volunteer firefighter, I've stood in the driveway with homeowners, watching as their house burned to the ground. It can be terrible and traumatic to watch your home or office seemingly self-destruct in slow motion, due to a spreading fire. Even if you have taken the precaution of installing smoke detectors, fire extinguishers, and other fire mitigation technologies, other tenants in your building or neighbors sharing common walls may not have done so. They add to your fire risk.

Plumbing Failures

We don't hear about plumbing failures in the news. In terms of disaster "sexiness," plumbing failures are pretty far down on the list.

Lest you think this is a risk not worth our time, I would encourage you to think again. A burst pipe in your office can flood a file room, conference rooms, your library, and other critical office space. The water can damage your furniture and computers. It can create a moldy office, requiring extensive remodeling.

Intentional Acts

Not long ago, the practice of law was considered to be at low risk of physical danger. However, in the last decade or so, we've seen an alarming spike in the number of incidents of violence in the workplace.

Workplace Violence

According to the Occupational Safety and Health Administration, the most extreme form of workplace violence, homicide, is the fourth-

leading cause of fatal occupational injury in the United States.[5] As lawyers, we are not immune.

Amarillo attorney Jeff Tormey and I once participated on a CLE panel on law firm disaster planning. In describing why our profession faced a growing risk of workplace violence, Tormey aptly stated, "Lawyers are in the business of ending things." In the process of "ending things," such as a marriage, a business, an employment relationship, or an estate, tensions and emotions can run quite high. As lawyers, we always need to be aware of the risks.

I'm sure that many of us, especially those of us with a trial practice, have had times when we feared we might be the victim of workplace violence. I myself have had witnesses rush toward me from the witness box during cross-examination and deponents come across the table while being interrogated on a sensitive subject, and I have received thinly veiled threats from disgruntled customers of my employer.

Again, we only need to search online for a few minutes to find heartbreaking stories of workplace violence in the legal profession. In 1994, a man involved in a civil lawsuit opened fire at a court reporter's office in Fort Lauderdale, Florida, killing a pregnant lawyer and a deponent and seriously wounding another attorney.[6] Here in Texas in 2005, divorce litigant David Hernandez Arroyo, Sr., fatally shot his ex-wife and wounded his son in front of the Smith County Courthouse, only then to engage police and other court officials in an extensive shootout.[7]

When I talk to lawyers from different types of firms about preparing for disasters, I find many firms have made preparations for the physical destruction of their firm or for damage to their computer sys-

---

5. "Safety and Health Topics: Workplace Violence," Occupational Safety and Health Administration, accessed May 18, 2011, **www.osha.gov/SLTC/workplaceviolence/**.

6. "2 Are Killed During Deposition in Florida," *New York Times*, May 28, 1994, **www.nytimes.com/1994/05/28/us/2-are-killed-during-deposition-in-florida.html?pagewanted=1**.

7. Maya Golden, "Tyler Shooting Suspect's Motive Believed to be a Custody Battle," *KLTV*, February 24, 2005, **www.kltv.com/story/2996186/tyler-shooting-suspects-motive-believed-to-be-a-custody-battle**.

tems. However, it's rare to find a firm that has made any plans for the possibility of workplace violence.

Along with the obvious physical injuries ensuing from workplace violence, the psychological injuries can be just as devastating and as long-lasting. Even when employees return to work, you can expect their productivity, for an extended period of time, to be a fraction of what it was before the incident. Further, depending on the type of practice a firm has, it may be difficult to continue as a firm, given the notoriety of the event.

Terrorism

In the days since 9/11, we are made acutely aware of terrorism every time we go through airport security, take a trip out of the country, or attend large gatherings that may be perceived as terrorist targets. A number of our colleagues were killed during those attacks on September 11, 2001, proving that our profession is not immune to the direct and indirect effects of terrorism.

It is my opinion that a firm in a city should be more prepared for the risk of terrorism than one in a smaller community. That is not to say that smaller communities would be immune from the direct effects of terrorism; however, given the nature of terrorism, larger cities with more people provide greater "shock value" as targets.

If you spend any time at all reading books on how to prepare for terrorist attacks, you'll learn quickly that there are a number of possible threats. These include large-scale explosions, bio-weapons, attacks using nuclear or chemical materials, or smaller explosions in crowded areas.

Here's some good news: the odds of dying in a terrorist attack in the United States are relatively small. Michael Rothschild, a former business professor at the University of Wisconsin, determined that a person's odds of dying on a hijacked plane—assuming that a plane is hijacked and crashed once per week—would be somewhere in the neigh-

borhood of 135,000 to one.[8] Compare that to the odds of dying in an automobile accident each year, which are in the neighborhood of 7,000 to one.

While I do think every business should have a plan in case a terrorist act directly or indirectly affects it, the good news is that many of the precautions we would take for other disasters would apply equally well to a terrorism scenario. In short, executing the basics of emergency planning will help you in any possible disaster situation, including terrorism.

Riots and Civil Unrest

Riots and civil unrest are quite similar to terrorism. Fortunately, they have less of an impact.

Historically, Americans riot over a number of things, including:

- Verdicts from criminal trials (unpopular with certain groups).
- Racial tensions among a city's residents.
- Meetings of world leaders, especially at conferences of the World Trade Organization.
- Championship games of our favorite professional sport franchises.

Afterwards, businesses not immediately affected can expect to be able to resume business fairly quickly, and without the psychological impact of a terrorist attack. However, businesses directly affected, whether from vandalism, police barricades, or lack of utilities, could be just as impacted by a small riot after a big football game as they would be from a larger national disaster.

8. Michael L. Rothschild, "Terrorism and You—The Real Odds," *Washington Post*, November 25, 2001.

Chapter 4

The Costs of Preparing for a Disaster vs. Not Preparing for One

I've always appreciated the story of Noah. The book of Genesis describes how Noah, commanded by the Lord to build a boat for his family and the Earth's creatures, received specifications and instructions on how to go about doing it.[1] I have to think Noah took a lot of ribbing about his ark . . . right up to the day it started raining.

The point we can all take from Noah's story is that it wasn't raining when he built the ark. Despite the fact that it took resources to build such a vessel, Noah believed he needed to prepare for a disaster and that such expenditures were necessary. Like Noah, we know a variety of disasters could affect our business. Are we willing to devote the necessary resources to mitigate those risks? What might it cost us if we don't?

While we can divide the costs of preparedness into a number of categories and subcategories, let's keep things simple and stick with

1. Gen. 6:14–16.

the three basic ones: *emergency gear*, *computer equipment*, and *insurance premiums*.

Emergency Gear

Many of the items on this list are what I call "common sense" ones. In fact, local fire codes and other regulations may require that an employer keep these items on the premises for life safety. Regardless of whether they are mandated by law, it's a good idea to keep the following items on hand:

- *Fire extinguishers.* A fire extinguisher rated "ABC" is sufficient to put out most fires. In residences, the National Fire Protection Association recommends a fire extinguisher for each level of the house, plus one for the garage. Your local building codes will likely have requirements for your office. Fire extinguishers normally cost between $30 to $60, depending on size and capacity. Make sure they get inspected or rotated as needed.
- *Plastic sheeting and tarps.* These can be purchased in large rolls at any home improvement store and will come in very handy when trying to protect files and other assets such as furniture, computers, and cabinets from water damage. Throwing the plastic sheeting over those items you wish to protect may be all that is required. Sheeting is an inexpensive and effective way to protect assets after the initial disaster. Keep in mind that your insurance policy will likely require you to mitigate your damages, which may require protecting your property from further water or sun damage. Plastic sheeting and tarps can help with this tremendously.
- *Duct tape.* You'll need a way to secure the plastic sheeting around your assets. Duct tape can be an essential tool in such situations. When I practiced in Fort Lauderdale, located on the Atlantic Coast, our plan to secure file cabinets from hurricanes

included wrapping the cabinets in plastic sheeting and using duct tape to keep the sheeting in place.

- *Basic first-aid kit.* Ideally, certain employees should have first-aid training to go along with the first-aid kit. Realistically, most people do not have any form of first-aid training. Given that, a basic first-aid kit filled with bandages, pain relievers, and antibiotic ointment can go a long way in dealing with minor injuries.
- *Rope.* I'm always amazed at how much rope costs when I go to the local home improvement store. Unfortunately, there are very few good substitutes. Rope can be used in a number of ways, including to secure office equipment in place and to affix plastic sheeting over furniture. Keep enough on hand to secure furniture and file cabinets.
- *Plywood sheeting.* We've all watched cable news or the Weather Channel reporting from a beach location just before a hurricane arrives. Inevitably, these crews report from the local home improvement store where residents purchase large quantities of plywood sheeting to board up a house. In many cases, these residents pay above market price or are unable to buy any plywood sheeting at all because there's been a large run on supplies. Every time I see these reports, I ask myself, "Why didn't they buy the plywood months in advance? They know they live in a hurricane-prone area; sooner or later they were bound to need it." I encourage you to not be the person who tries to buy plywood and other storm supplies at the last minute. You know you're going to need it if you live in a storm-prone area; go ahead and purchase it now while the supplies are reasonably priced and available.
- *Flashlights.* The lowly flashlight can be the ultimate survival tool. In a power outage or in heavy smoke from a fire that is engulfing hallways, a flashlight can literally save your life. I always carry a flashlight on me—a Surefire Outdoorsman model. As a bonus, flashlights are dirt-cheap. Get several for your office.

- *Smoke detectors.* Most building codes require smoke detectors. Depending on your situation, you may need to provide additional smoke detectors for additional coverage. Like flashlights and first-aid kits, these items can be purchased inexpensively at home improvement and big box retail stores.
- *Weather radio.* The National Weather Service broadcasts weather information twenty-four hours a day, which can be heard on specially-built radios. In addition, most of these radios automatically turn themselves on in the event of severe weather. Having a weather radio will provide you with relevant weather information for your area. (I personally own six such radios—three free-standing weather radios, one alarm clock with built-in weather radio, one handheld radio for my truck, and one that is built into my ham radio walkie talkie. Yes, this makes me a geek—*a well-prepared geek*.) If you choose to purchase a weather radio, I strongly recommend that you buy one with the SAME programmable feature. This function allows you to program your radio for certain types of threats in your county. That way, you don't receive extraneous alerts for situations in remote locations.

Additional emergency gear items that a business should consider keeping on hand are listed in Appendix A.

Computer Equipment

Buying certain computer equipment as part of a disaster preparedness plan makes good sense. Helpful technology for contingency planners that was out of financial reach five to ten years ago is now quite affordable for most businesses. In regard to computers, expenditures to prepare for disasters fall primarily into two categories: backup hardware and uninterrupted power supply.

A medium-sized firm can acquire enough computer backup hardware (such as external hard drives and flash drives) to back up all of its important files for a few hundred dollars. Uninterrupted power sup-

plies, which provide battery power during times of power outages, run anywhere from $50 (capable of running a small computer for fifteen minutes) to hundreds of dollars (capable of running a computer for close to forty minutes). For run times longer than these figures, most people would opt to use some sort of electrical generator.

Cloud Computing

More businesses are turning to cloud computing to back up their critical software and data. Lawyers should know the pros and cons of using a cloud computing arrangement before electing to use such a service.

Attorney Ronald L. Chichester defines cloud computing as "the placing of data and/or a software application onto a (third party) server that is accessible via a wide area network, such as the Internet."[2] Think of cloud computing as a server somewhere off site, owned by another company, where you and thousands of your best friends store data and backed-up software. A number of companies provide cloud computing services, often marketed as "online backup services," to all sorts of businesses.

Clearly, cloud computing has some distinct advantages. For example, you can customize your backup schedules, making them truly a "set it and forget it" system. The backups can be run automatically, so there's no need for you to remember to do the backup. Cloud computing provides a timely and reliable means of backing up critical data in the event of a computer malfunction or some sort of calamity befalling your office.

Additionally, cloud computing services can be reasonably inexpensive. According to Chichester, using cloud computing services reduces infrastructure and training costs considerably since the user need not purchase and maintain expensive, complicated software packages. Such services charge a regular fee for a given amount of storage space on

2. Ronald L. Chichester. "Litigating on the Clouds." In *Perfecting Your Practice 2010*. Austin: State Bar of Texas, 2010.

their server.

Of course, lawyers should also fully understand the drawbacks to using such an arrangement. Chichester outlines three main concerns lawyers should contemplate. First, "the service provider may store your information in a proprietary format, making it difficult to 'liberate' your data for backup, transfer, or production during discovery." Next, "the provider may assert ownership of the data by virtue of contract or copyright." Finally, "the service provider can interrupt access to your data at any time."

While you can find a number of articles that go into detail about the hazards of cloud computing arrangements, I believe the following is a fair summary: people who use such services often subject themselves to certain risks, including that the vendor could go out of business, claim copyright to your data, or create compliance issues with laws such as chapter 521 of the Texas Business and Commerce Code. *See* Tex. Bus. & Com. Code §§ 521.001–.152. Some people in the information systems industry have expressed concerns about the cloud computing concept. Fears over loss of control and security of data maintained by cloud environments have prompted some experts to advise clients to think twice about using such technology.[3]

Within a legal environment, similar fears might arise. Putting sensitive data regarding your clients on a server you do not control, accessible to other users who are also putting their own data on the server but ostensibly cannot access the data you might put there, ought to raise some ethical concerns as well. The State Bar of Texas, as of this book's publication, has not issued any formal guidance on this topic. But if you are an attorney using a cloud computing arrangement, you should carefully scrutinize any agreement with the cloud computing service to make sure that adequate safeguards are in place to protect the privacy of your data and that you retain the ownership of any data parked on its server. You should also do your due diligence to determine the long-term reliability of the vendor.

---

3. Ericka Chickowski, "Cloud Creates SIEM Blind Spot," *Dark Reading*, October 27, 2010, **www.darkreading.com/security-monitoring/167901086/security/security-management/228000206/index.html**.

Insurance Premiums

Insurance premiums for a law firm will vary on a number of factors, including:

- Whether the firm owns its office space or leases it.
- The amount of tangible assets owned by the firm, such as furniture, office equipment, and vehicles.
- Whether the firm opts to carry business interruption insurance.
- For malpractice coverage premiums, the type of practice, the number of attorneys, and the prior loss history.

Insurance coverage warrants an extended discussion itself, which you can find in chapter 9. Your insurance agent is the best source of information on what coverages you need and what it will cost your firm.

The Costs of Not Preparing

Without question, a law firm can save a lot of money if it doesn't prepare. Insurance premiums, equipment to back up computers, and emergency gear all cost money. As discussed above, you'll likely have a long shopping list if you plan to start making preparations for disaster.

But what are the costs of not preparing for disaster? Of course, each law firm's response to this question would be different. However, I can think of three areas of potential loss that each firm should consider when analyzing the costs of preparing versus those of not preparing for a disaster.

1. *Loss of income.* If a disaster, large or small, keeps you from generating revenue and handling accounts receivable for a period of six to eight months, could your firm survive? On a personal level, could you afford to pay your family's bills? Could you afford to keep your key employees during a time where no income is coming in?

2. *Loss of market share.* If you are unable to take care of your clients, some other law firm will. As professionals, we don't generally like to think that other attorneys will go after our business. However, clients have legal needs, and they will go to those who can meet those needs.

3. *Loss of physical assets.* What will it take to replace computer hardware, furniture, office space, and paper files? To replace all of these items with new or slightly used products could cost a sizable sum of money.

In addition, an increasingly relevant concern is that firms might face liability for not meeting an ethical obligation of preparing for disasters. Most bar associations seem to take a "reasonableness" approach in determining whether a lawyer has met ethical obligations in protecting client information and property from disaster. As long as a lawyer has taken reasonable steps to protect client data and property, ostensibly the lawyer would not face any liability under the rules of professional responsibility for loss of client data or property. This, of course, raises the question: "What's reasonable?"

In this age of information security issues, one could argue that the standard of care rose dramatically in this area some time ago. Florida lawyer James Keim wrote an article in the *Florida Bar Journal* in which he challenged the traditional notions of a lawyer's ethical duties with regards to preparing a law office for disaster. Keim sums up his central argument with this question to the profession:

> If an attorney has purchased hurricane shutters to safeguard and protect a personal home and its contents but has failed to do so to protect his or her office and the clients' property contained therein, has the attorney acted unethically? Likewise, has the attorney's conduct constituted negligence given that he or she failed to act even though the attorney possessed knowledge of a foreseeable risk of harm to the client's property?[4]

4. James Keim, "Law Office Disaster Preparedness: The Liability and Ethics of Attorneys," *Florida Bar Journal* 80, no. 5 (May 2006): 27.

To support his argument, Keim relies on the Rules of Professional Responsibility as they pertain to the safekeeping of property. *See, e.g.*, Tex. Disciplinary Rules Prof'l Conduct R. 1.15, *reprinted in* Tex. Gov't Code Ann., tit. 2, subtit. G, app. A (West 2005) (Tex. State Bar R. art. X, § 9).

Keim notes that the Florida Supreme Court, in interpreting the rule requiring Florida lawyers to safeguard property, held that "the responsibility of preserving client property rests in the hands of both individual attorneys and the legal profession itself."[5]

In a personal communication, Keim elaborated:

> This duty of preservation is not a novel concept to lawyers or the legal profession as a whole. It has always existed. We are simply applying this traditional concept in a new context—disaster planning—and in doing so, we are bringing the legal profession in line with standards long embraced by the financial, insurance, and healthcare industries. . . . If members of the insurance, financial, and healthcare sectors are capable of foreseeing and planning against losses occasioned by disaster, why should we hold lawyers or the legal profession to a lesser standard? Indeed, we are specially trained and taught to analyze risk and assist our clients in avoiding harm, financial or otherwise. Foreseeability of harm may give rise to a legal duty to act to protect client property and interests. If a lawyer carelessly, recklessly, or willfully ignores that duty, civil liability could ensue.[6]

Keim added that the standard of care lawyers must meet to prepare their offices for disaster will only rise as more lawyers write about, bar associations study, and courts address the subject. Keim told me:

> At the present time, without written uniform standards or guidelines to assist lawyers in determining what actions are adequate and reasonable in preparing for disaster, it is dif-

5. *Florida Bar v. Ward*, 599 So.2d 650, 652 (Fla. 1992).

6. James Keim, e-mail message to author, December 11, 2010.

> ficult to pinpoint what the standard of care would require of individual lawyers and the legal profession. For now, that question is likely to be answered on a case-by-case basis. Geography and local customs will certainly play a role in the determination. For instance, a small coastal law firm in Texas faces different threats in comparison to a law office in El Paso. Yet, common threats such as fire, flood, tornadoes, and theft are readily identifiable in both locations.

To be sure, any business would have to factor in the risk of a particular catastrophic event when making determinations on how much to spend on disaster preparedness. For example, it would not make sense to spend six months' worth of revenue to purchase an item or an insurance policy to protect against a risk that would likely only occur once in a thousand years. But as we'll see in subsequent chapters, the potential risk of business-damaging disasters makes disaster planning, and acquiring the right tools to manage disasters, essential.

One more point on expenditures—remember that these acquisitions are often one-time expenditures. With any luck, you won't be buying fire extinguishers or duct tape yearly. Hopefully, you won't have to buy external hard drives every six months. Many of these items ought to last you for several years. Thus, the long term cost of preparing, spread out over time, is much smaller than you might think.

Is it time to start building your ark? Since you're reading this book, it stands to reason that you feel the need to get better prepared. At the end of the day, only you and your business partners can determine whether the cost of preparing is worth the expense to avoid what could ultimately be a far greater harm.

Chapter 5

Incident Response, Business Continuity, and Why Rule Books Don't Apply

One of my favorite ways to relax while working in my home office is to play a Bob Ross DVD in the background. For those of you who may not watch much public television, Bob Ross became an international sensation with his show, "The Joy of Painting." Although he passed away in 1995, dozens of television stations still schedule his show, which continues to draw a huge audience. Ross encouraged people to paint by using a litany of folksy sayings. He regularly told viewers, "We don't make mistakes; we have happy accidents." With that philosophy in mind, he took a blank canvas and churned out a painting in a mere twenty-seven minutes.

Like painting a picture, dealing with crises is an art. Much like an artist starting with a damaged or defective canvas, a disaster manager is handed a bad situation and implicitly told to "fix it and make it all pretty again." In doing so, the manager must understand *incident response* and *business continuity*.

Incident response is the method by which an organization copes

with a variety of emergencies. More succinctly, incident response stops the bleeding—literally and figuratively. An organization's incident response plan will outline steps it will take to protect employees, customers, and facilities. Business continuity, on the other hand, is the process organizations use to get back on their feet and continue their missions. Once the bleeding has stopped, the organization can figure out how to resume as a business.

Although people often confuse the two terms, each one refers to a different type of action plan. Incident response could also be called *emergency response.* The immediate steps a business takes to get people and property to safety are the essence of incident response. Those working in incident response must be able to think and act quickly, under extraordinary pressure, and in very emotional situations.

Business continuity efforts, while equally important, center on running a business without the normal business infrastructure. While this, too, can be mentally draining, it does not have to be done at a frantic pace or in a dangerous situation. Business continuity planners must determine how to run an office without a traditional office space, without the usual office equipment and files, and with less than a full staff, while still meeting customers' expectations.

Think of it this way. Suppose you're preparing for a dinner party one evening, and the guests are slated to arrive in an hour. You then find that your three-year-old child has spilled nail polish all over the dining room where the meal will be served. At that moment, you have two concerns: getting the polish up before it dries and determining where the guests will dine if the dining room cannot be used.

Your first concern would be handled by an incident response plan. Wiping up the fresh polish, racing to the computer to find an Internet video describing how to remove nail polish from carpet and upholstery, and disarming the three-year-old of his or her arsenal of colorful (and permanent) goo—these are the tasks the incident response plan contemplates and resolves. Determining whether the dining room is usable and, if not, calling up friends to borrow card tables, moving furniture around the den to create a temporary dining room, and coming up with a sound bite to explain to guests why they are dining on card tables in the den—

these activities exemplify business continuity efforts.

Incident response and business continuity efforts may take place simultaneously. If you have enough help in your firm, one or more persons might be tasked with incident response efforts while one or more handles business continuity operations. Regardless of whether certain people are designated for incident response and others to business continuity or if all emergency team members share both types of responsibilities, it's critical that you understand what must be done immediately after the incident and what tasks can wait a few days. Otherwise, you will quickly become overwhelmed and possibly paralyzed, incapable of doing anything.

Understanding the Incident Response and Business Continuity Environments

Take a moment and envision standing in your parking lot, watching your office engulfed in flames. Or maybe you're in your office when a staff person reports that a plumbing line in the ceiling has sprung a big leak, contaminating your files. In either event, we can assume a few things:

- Your stress level will grow exponentially in the following hours and days.
- Your staff will look to you for answers to a host of questions, ranging from "What are we supposed to do?" to "Does this mean we *won't* be having the office picnic next week?"
- The media may approach you, depending on the size of the incident, and ask for your comments.
- You may be forced outside of your building with your employees, at which point you will have to endure whatever weather conditions await you. In Texas, that can be anything from 100-plus degree heat to freezing drizzle to severe thunderstorms. Meanwhile, things you and your staff need—from

computers and files to car keys and cell phones—may be stuck inside the building, completely inaccessible and possibly destroyed, depending on the disaster.

- Your calendar—both professional and personal—just imploded for at least the next week, maybe longer.

Welcome to the incident response environment. It can be an extremely stressful and lonely one. You mitigate the stress by planning for the worst *now*, rather than hoping it doesn't happen. Here's the good news: planning for incident response and business continuity need not be time-consuming or costly.

As we move forward, I want you to remember what I call the Incident Response Keys to Victory. These include:

1. *Decide, don't hide.* It's often easy to become overwhelmed by the situation. When this happens, people find it hard to make a decision and end up hiding in the crowd. Condition yourself to step up and make decisions on how to proceed.
2. *Know that you don't know.* You will need to make decisions when you don't have perfect information. Some of us tend to freeze up in this situation, claiming that no decision can be made until we have all the facts. Know that you will have to do just that. Often, a bad decision is better than no decision at all.
3. *Don't let "perfect" be the enemy of "good."* A surgeon once explained to me that young surgeons sometimes end up doing harm by trying to improve upon something that is already working well. Often we do more harm in the pursuit of perfection when "good" is "good enough." If you start handling an incident and your plan seems to be working effectively, think twice about altering the plan. Put another way, "If it ain't broke, don't fix it."
4. *Communicate, delegate, isolate.* These are some of the "*ates"* of incident response. You cannot over*communicate* with your team. They need information to let them know that you have a game plan and that it's being implemented. Share with them

what you know, and if you don't know something, tell them that too. Give them something to do; *delegate* various tasks to others, such as taking roll, arranging for transportation home, and talking to the insurance company. Then *isolate* yourself; intentionally make yourself unavailable to everyone. You cannot possibly manage the crisis with people running up to you every minute with concerns about how they are going to get home and where they should report to work tomorrow.

5. *Don't be afraid to say "Houston, we've had a problem."* Astronaut James Lovell uttered this famous phrase during the Apollo 13 mission. When the problem occurred, Lovell didn't hesitate to call for help. Similarly, when the incident occurs at your office, you need to be prepared to call for help. This could mean calling 911, your property management company, your insurer, or your office cleaning service. Don't delay—delegate someone on the scene to start making calls and get help rolling your way.

Back to Bob Ross. Whenever the paint or the canvas threw him a curve, he dealt with it. You will have to do the same thing. Be prepared now to think creatively and innovatively to solve the problem. Start asking yourself and others, "What would we do if [insert some disaster that might affect your office]?" The more you practice this, the better prepared you will be for the real thing. Because when it happens, your "rule book"—how you've been running your office up to this point—has just gone out the window.

Chapter 6

First Steps in Creating a Preparedness Plan

As Supreme Commander of the Allied Expeditionary Forces during World War II, General Dwight D. Eisenhower spent a fair amount of his time planning. The most critical battle plan of his career took the Allied forces to the beaches of France during the D-Day invasion. President Richard Nixon attributed the following as one of Ike's favorite maxims: "In preparing for battle, I have found that plans are useless, but planning is indispensible."[1]

That seems like a strange thing to say, doesn't it? Much of this book discusses the need for plans, the need to have the plans handy, the need to have the plans updated regularly, the need to test the plans, and so on. If plans are useless, why is planning indispensible?

To be sure, much of disaster planning is purely academic. Once we understand the basics of our insurance policies, the threats we face, and why we need to prepare, we've spent a fair amount of mental energy.

1. Richard M. Nixon, *Six Crises* (New York: Warner Books, 1979).

However, the truly difficult task, from an intellectual standpoint, is the creation of the disaster plan itself—the "planning" part Ike mentioned. It's during the planning process that you identify strengths, weaknesses, and contingencies that will help you overcome the unexpected.

There are a number of ways to go about creating your plan. My advice to you is pretty simple—find one that appeals to you and then use it. But unless you borrow someone else's plan, or hire an expert to create one for you, you will be making your own. In the coming pages, I'm going to outline a process on how to make your own disaster plan.

Playing the "What If" Game

Grab a pen and two pads of paper. If you're doing this by yourself, find a quiet time and place in your office to begin the process. If you're doing it as a team, make sure the team is focused and without distractions for the next hour or so. By following the steps listed below, you should find that your efforts will yield a quite workable disaster plan for your office.

1. At the top of one of the notepads, write the word "Procedures." On the other notepad, write the word "Stuff."
2. On the "Procedures" notepad, list all the possible things that could go wrong in your office. For each item, create a way (and if you can, more than one way) to alleviate that situation. For example, suppose you wrote down "plumbing failure floods the office." Alongside that entry, write down your options to get things back on track. Options might include identifying an alternative workspace to use while the mess is being cleaned (don't forget to identify what that place might be!) and contacting a remediator to repair any waterlogged hard files and a computer repair outfit to repair damaged hardware.
3. Every time you come up with a problem and a procedure to fix it, take your "Stuff" notepad and list the things you would need to implement your procedure. In the previous example, some of the stuff you might need could include plastic sheet-

ing, a wet/dry vacuum (which could be purchased relatively inexpensively or rented from home improvement stores), and duct tape. The list should include the phone numbers of various vendors who could help you after a disaster.

4. Continue to do this over and over again until you're convinced you've captured every conceivable scenario, both large and small.

5. Once you're satisfied that you've completed your lists, go back through them and ask yourself, "What would happen if my proposed solution became unworkable?" For example, suppose the ensuing water damage from the plumbing failure made the file room unsanitary and thus uninhabitable, as well as making the contents of the room unsafe to handle. What would your procedure be for that situation?

6. Once you've come up with some workarounds for when your first response to a problem doesn't work, you're ready to start writing your "preparedness story." Your preparedness story need not be long; a page or two should more than suffice to cover all the bases. The preparedness story is simply a synopsis of how you would handle disasters. Your story may sound something like this:

> To ensure business continuity, we regularly back up all of our computer hard drives with portable hard drives, which we remove from the premises on completing the backup. We've acquired several recovery supplies, such as plastic sheeting, rope, duct tape, caulk, trash bags, and a wet/dry vacuum. We keep some of these supplies on site for a rapid response; other supplies, such as our wet/dry vacuum, belong to one of the attorneys and remain at his house.
>
> In the event we need to relocate somewhere else while our office is being repaired, we've established an agreement with another law firm a few blocks away allowing us to use their unused office space and conference rooms until we can acquire additional space.

> To ensure that we keep our clients apprised of our situation, we've created a standard notebook, shared with key attorneys, setting forth the instructions on how best to advise our clients of our new office space and contact information. The checklist in that book also reminds the attorneys to notify the local courts where we practice of our situation and how best to contact us.
>
> We expect employee morale issues might result from a disaster. To that end, we have appointed two attorneys, noted for their people skills, to act as the primary points of contact for our associates and staff.

7. Once you've written your preparedness story, share it with others. Remember, there's no attorney-client privilege here; your plan should not be treated as proprietary information. Have your attorneys and other law firms' attorneys and staff review it for you and offer suggestions. With any luck, your efforts may encourage them to begin their preparedness efforts as well.

Creating Your Incident Response/Business Continuity Team

I could write pages explaining why an incident response/business continuity team is essential. Instead, let me summarize it in one sentence: *You cannot do everything yourself*. There is too much to do after a disaster, with too few resources, by people who are not trained in emergency management and disaster recovery, for one person to do everything. Thus, you will need to create a team of people to help respond to disaster.

Many of you in small firms will feel that you do not have enough people to create a team. Note that the team need not be large; however, it does need to involve more than one person, unless you are the sole employee of the firm. Even then, you may find it helpful to conscript family members or a temp agency to help you.

There are a number of ways to organize your team and divide up responsibilities. It's not my goal to prescribe one method over another; rather, you need to figure out what works best for your business. Here are some things you might want to consider:

- Who in your office performs well under pressure? Such people, regardless of their skill sets, make good team members.
- Who in your office is a "people person"? Someone will need to communicate with the firm's employees on a regular basis, fielding their questions, reassuring them, and encouraging them to focus on the various tasks at hand. If you have someone who is adroit with people issues, that person would undoubtedly be a great asset to your team.
- Delegation and clear communication are critical. Certain people need to be given certain tasks, based on their abilities and skill sets. Further, simply telling your team members to "call the insurance agent after the disaster" may not be sufficient to get it done. On the other hand, specifying that "Ryan or John will call the insurance agent" narrows down who will have that responsibility.
- It is important to share knowledge and to possibly appoint backups for the various team members. All members of the team should have a copy of the plan. It may be that some members of the team, for any number of reasons, will not be able to participate in the response or recovery of the business. If they are injured or cannot get to the office, for example, someone will have to fill in for them. If everyone has a copy of the plan, then each team member will have at least a working knowledge of what the other team members are supposed to do.

Compiling Your Roster

Once you've identified the team's members, it's time to record this list. On a sheet of paper, create your "roster." Your roster should list all of your team members and all of their responsibilities. It will also tell

the reader what your business will do in the event of an emergency. For example, your roster may look something like this:

> Our business's incident response/business continuity team consists of Jeff (principal), Tammy (office manager), and Jill (secretary). The firm's managers will activate the team if they decide a situation warrants it.
>
> Once activated, this team has full responsibility to manage all operations of the firm. Jeff, as a partner in the firm, will be in charge of the team's efforts. His primary responsibilities are, but are not limited to—
>
> 1. advising the courts of our firm's situation, if warranted;
> 2. advising clients of our situation, if warranted;
> 3. identifying alternative workspace for temporarily relocating the firm's operations, if needed; and
> 4. insuring that timekeepers continue to maximize billable hours and receivables during the crisis, to the extent possible.
>
> Tammy, as office manager, will be responsible for all human resource issues involving nonattorney employees. She is also authorized to instruct the firm's staff to take whatever remedial or mitigation efforts are necessary to protect the firm's information and physical assets. She has a budget of $5,000 to secure any needed resources, such as office supplies, vendors, and staff overtime. She need not seek management approval to use any money budgeted during the time the team is activated. Any expense items over $2,000, however, must be approved by firm leadership.
>
> Jill will act as team leader for all support operations. She will marshal and manage staff employees who are able to come to work and who can help carry out the necessary tasks of mitigation.

Creating Your Own Procedures

Simply put, procedures that are not written down don't exist. You will not have the time nor the frame of mind to remind people of all of the necessary procedures in the middle of an emergency.

The good news is that there are only two rules in creating incident response/business continuity procedures. First, write your procedures simply so that anyone can understand them. Bear in mind that it may be a sixteen-year-old child of one of your employees who is pressed into action to help the firm recover. That individual needs to be able to look at the plan, read a portion of it, and then have a full understanding of what has to happen. *You cannot write a plan that is too simple.* We are not trying to insult anyone's intelligence here; however, we have to be mindful that we're dealing with a stressful situation and with individuals who are not trained in incident response or business continuity.

Second, remember that the scenario you actually face will be different from any scenario you may have concocted, so make your plan flexible. Military history is replete with battle plans that were changed early on in the fight. That's because it's simply not possible to forecast and predict with any accuracy every single variable. For example, if your plan calls for you to move your office operations into a conference room of another law firm ten blocks down the street, one of the implied conditions would be that the other law firm's office be accessible. However, if it's difficult or impossible to get to the other law firm, that part of your plan isn't going to work. So for that scenario, it would be good to have multiple locations in mind to meet your firm's needs.

Now that you've created the framework of a disaster plan, you are in a far better position to deal with whatever might come up. It's this planning process—and not the plans themselves—that will better prepare your firm and your people for the prospects of a disaster.

Chapter 7

Anatomy of an Incident Response/Business Continuity Plan

So what does a completed disaster plan look like?

It looks like whatever you want it to look like. I know that's not a good answer, but it's important that you understand that it's *your* plan, not mine. So customize it to make it do what *you* need it to do.

To get you started, I am going to walk you through one example of what you might expect to see if someone handed you a plan for your business. For this discussion, the hypothetical firm has roughly ten attorneys and ten staff employees. The firm is located in Austin, which means it does not have coastal exposure but could still feel the effects of a hurricane hitting the Texas coast. A fully developed sample plan can be found in Appendix D.

Plan Format

We hit our first question in the decision tree right away. Do we use hard copies of the plan, soft copies of the plan, or both?

Hard Copy Pros and Cons:

- Hard copies need no electricity or technology.
- Hard copies take up space.
- Hard copies are a pain to update since you have to change every single copy.
- Hard copies provide no inherent security as to their contents (which may be desired as some portions of the plan might contain proprietary information, such as employees' addresses and phone numbers).

Soft Copy Pros and Cons:

- Soft copies can be put on a thumb drive and attached to a keychain for ease of use.
- Soft copies are easy to update.
- Soft copies can be password protected (to maintain the security of any proprietary information contained in the plan, as mentioned above).
- Soft copies require computers and electricity to access.
- Thumb drives and external hard drives can crash, making the plan inaccessible.

My personal bias is for hard copies. I place the hard copies in red folders so that they stand out. Further, when I tell the incident response or business continuity team to check their "red folder" for this or that, there's no question what I am talking about. These red folders have never failed to boot and have never been accidentally deleted or made inaccessible due to a software virus. Plus, I tend to be a bit "old school" in that I prefer holding paper in my hand when I absolutely need critical information. Many of you, however, likely shudder at the thought of a hard copy. Do what makes sense for you. Whether you use hard or soft copies to record your plans, here are several suggestions about what they should contain. Again, you can see examples of some of these items in Appendix D.

Emergency Instructions for Employees

Each member of your organization should have a short, half-page memo detailing what to do in case of fire, severe weather, or other emergency. It should contain the emergency contact numbers for them to call to get further instructions in the event of an emergency.

Why put this in your red folder? I do so because I want to have a copy of whatever instructions my employees have and are hopefully following. Everyone's having a copy means we are all on the same page.

Emergency Contact Information

You need to know how to get in touch with your employees, preferably through multiple means. This means having not only their names, phone numbers, and physical home addresses, but their "in case of emergency" contacts as well. The growing practice of abandoning traditional landlines at home in favor of a cell phone means we have one less means of getting in touch with our employees. On the upside, having the ability to send text messages adds a new dimension to our emergency communications.

Phase Checklists

When I started developing a disaster plan for my legal department, it dawned on me that we needed to have some protocols to follow both pre- and postdisaster. I drew upon my extremely limited computer training in high school—learning the old BASIC programming language—and wrote out steps to follow and in what order. Grouping these activities into phases makes it easier for everyone to know what activities need to be done and when to do them. For example, if it's time to "implement phase 2 protocols," you simply open up your red folder, turn to phase 2, and read the checklist.

Outline of Ongoing Precautions

What are you doing daily or weekly to prepare for a disaster? For example, what's the plan for backing up computer data? How often do you review the red folder to update it? Outline your ongoing precautions so you can have a clear list of those activities.

Special Considerations for Certain Scenarios

Some scenarios don't lend themselves well to the phase checklists mentioned above. Catastrophic events come to mind. Write out special instructions for those scenarios that require it.

Solutions for Possible Problems

A disaster is a disaster is a disaster. Many disaster planners would cringe at that notion, but I think it's quite true. For example, if your building is destroyed, does it matter if it was destroyed by fire or weather? If you're having communications issues with your staff post-disaster, does it matter if those issues were caused by a plumbing failure requiring an office evacuation or a shooting in the work place? You will find that a number of the problems you are trying to solve are identical across the spectrum of the possible disasters that could affect a law office. Take advantage of that and prepare some suggestions on how to handle common problems that might come up postdisaster.

Identification of Alternative Work Sites

Quick—the building just blew up. Where do you plan to go to work tomorrow? Think about alternative work site issues now and have the possible solutions written down. If you have arranged with another busi-

ness to partner with them in the event of a disaster to either business, be sure to put in the plan where that business is located. In addition, think about where you plan to receive mail and to fax documents, if needed. Write down the names and locations of the places where you can do those things, too.

Note on Personal Items

I suspect most of us do this to one extent or another already. I encourage everyone to keep some basic supplies at work—medications, personal hygiene items, high energy snacks, and maybe even a change of clothes. I keep a razor at work as well, in case we need to "shelter in place" for a given period of time. I also keep a small poncho, a first-aid kit, a powdered sports drink mix, and a few other items to make a disaster more manageable.

Plans for Accountability/PAR

In the aftermath of a disaster, one of your first orders of business will be to determine the status and location of your staff. First responders often refer to this as taking a *personnel accountability report* or "PAR." Taking a PAR is a high priority. Think about how you want to go about doing that. Also, for offices where attorneys regularly leave the office for meetings, court appearances, depositions, and travel, how will you determine their whereabouts? Work through those issues and incorporate them into your red folder.

Launch Code Cards

Every U.S. president has access to the nuclear weapons launch codes. These codes appear on a card kept constantly close to the president by the military. You should also have your own version of a launch code card available to you at all times.

Your launch code cards enable you to "launch" your incident response or business continuity plans. I created launch code cards for our emergency responders, giving them the basic information they need to get started in the crisis management process. A launch code card might look something like this:

[Side 1] Emergency Contacts			
Insurance Agent:	[phone number]	Computer Support:	[phone number]
Neighboring Law Firm:	[phone number]	Office Manager:	[phone number]
Remediation Company:	[phone number]	Managing Partner:	[phone number]
Court Reporting Firm:	[phone number]	Accounting Firm:	[phone number]
Rental Car Company:	[phone number]	Office Supplies:	[phone number]

[Side 2] Incident Response First Steps
❒ Call 911 if necessary
❒ Ensure employees are safe/complete PAR
❒ Contact insurance company
❒ Notify absent employees
❒ Take mitigation steps if possible
❒ Advise firm leadership
❒ Arrange to get employees home if needed
❒ Notify court reporters/courts of situation if needed

This launch code card will help you get your head into the game, so to speak. I would suggest making it a credit card-sized list, and then laminate it. Put it in your wallet or purse so that it's always with you.

Appendix E includes multiple sets of sample launch code cards. Feel free to photocopy the page of cards, fill in the necessary contact information, and distribute the cards to key players in your firm.

Chapter 8

Updating and Testing Your Plans

Every Christmas, I make the pilgrimage to my family's farm in Tennessee. During one such trip a few years ago, the weather forecast predicted that an ice storm would hit the area the day after I planned to return to Texas. In preparation for the storm, my dad and I went to the barn to retrieve the generator, which my parents often use when the power goes out. We carried it to the house, fueled it up, and tried to start it . . . and tried, and tried, and tried. I asked my father how long it had been since he had started it. He thought it had been a while—several months. He eventually got it to start, after much effort.

It's simply not enough to write a plan, share it, stick it in a folder, and place the folder in a file cabinet somewhere. Like my dad's generator, the plan must be regularly tested and maintained. The number of small changes to your workplace that could have a major effect on your plans include:

- The departure of key employees.
- The arrival of new employees with special needs or skill sets.

- A change in tenants in your building, which may increase certain risks to your firm.
- A change in office space.
- A change in the home address or phone number of an employee.
- A change in the areas of your firm's practice.

Thus we need to focus on two key concepts—*updating the plan* and *testing the plan.*

Updating the Plan

Years ago, I maintained a business continuity plan for my legal department. During a winter weather event, I tried to contact several employees to let them know the latest situation. I quickly found that many of them had changed their cell phone numbers or had moved from their last addresses. While this wasn't a critical situation, it would have been much more stressful if I had really needed to get into contact with them. As a result of that event, I put a note on my calendar to verify the home address and contact information for every department employee on a quarterly basis. The updating process took only a few minutes and was well worth the time spent.

Some aspects of your plan will change less frequently. But when those changes do occur, you need to update your plan. Using the list of possible changes above, let's review how they might impact your disaster plan.

The Departure of Key Employees from Your Firm

Hopefully, your business won't have a mass exodus of employees, requiring incident response and business continuity duties to be reassigned. But even if only one key employee departs the firm, you may be faced with a gaping hole that needs to be filled both quickly and correct-

ly. One easy way to do that is to have a backup person assigned to each key role in the plan. If, for whatever reason, the assigned person cannot fulfill the role, the backup takes over.

A backup is not only a good way to hedge against the risk of having a key employee leave the business, it can also be a life saver if the assigned person is unable to do the job in the event of a disaster. If the firm's office manager, Tammy, is supposed to head up incident response during the disaster that just hit your office, but Tammy is on a cruise ship in the Caribbean, blissfully unaware that the office is imploding, someone needs to step up and take her place. If you designated a backup in advance and had that backup trained to do the job, your recovery will go more smoothly.

The Arrival of New Employees with Special Needs or Skill Sets

In a diverse workforce, we may encounter a number of people with certain physical or mental limitations. These limitations may require us to make accommodations to ensure their well-being during a disaster. For example, if the firm hires employees with mobility issues, your team will need to determine the best way to assist these individuals in the event of a disaster.

Employee changes in your plans need not always be a challenge. I've practiced law with a former firefighter, a Vietnam veteran, a former JAG officer, an ordained minister, a Boy Scout troop leader, a former state trooper, an Iraq war veteran, and a former Army helicopter pilot. As you can imagine, each of those individuals possessed a number of valuable skills and training for dealing with disasters. If a new employee with some similar type of past experience or current hobby joins your firm, the addition of that person to the team might add a new dimension to your disaster response.

A Change in Tenants in Your Building

I'm willing to bet that this topic is rarely on the radar of most people tasked with incident response or business continuity efforts in any business. Suppose for a minute that the empty office space down the hall from you eventually becomes the new home to a federal law enforcement agency, such as the FBI or the DEA. Or perhaps the IRS sets up shop down the hall. Or maybe it's Planned Parenthood. Any of these organizations might draw the unwanted attention of a protestor who could take violent action against the facility or its occupants—which might include you.

Another possibility is that a new tenant could set up shop whose work with chemicals or hazardous equipment increases the risk of fire or contamination. Many high-tech companies use equipment that contains dangerous chemicals or biohazards. These businesses may seem very nondescript and have a seemingly pleasant stream of visitors to their office space. You might not have any idea of what risks lie within their walls until something in their office space goes horribly wrong.

A Change in Office Space

This fundamental change—moving from one office space to another—necessitates a complete and thorough review of the entire plan. Here are just a few possible scenarios: moving from leased space to owned space; moving from a small office center to a downtown high rise; relocating from a suburban area to one in the center of the city. Each of these changes can create many challenges. (Although, of course, each could also eliminate some of the challenges you faced in your old space, as well.)

Businesses move to different office spaces for a myriad of reasons. I would urge you to consider several disaster recovery factors in addition to your other search criteria:

- If a major disaster hit the building while we were at work, how easy would it be to leave the building?

- Who are the current occupants of the building? Does the building have any restrictions on the types of businesses that can lease space in it?
- If there was a major disruption in the local infrastructure, would the building still be fairly accessible?
- What is the local crime rate around the building?
- How is the building constructed? Is it made of steel and concrete or is it a restored home originally built a hundred years ago?

Moving taxes even the best of us. It's a stressful time, filled with confusion and frustration. It's absolutely critical, however, that you plan to rethink your disaster plan once you have moved into your new office. And if you want to be super-prepared, think about how you would handle a disaster during the moving process, which would send your stress level off the charts!

A Change in the Home Address or Phone Number of an Employee

As I noted above, something as simple as a change in a cell phone number can result in losing contact with an employee during a crisis. Set up a regular schedule for updating everyone's contact information. I think a quarterly review is sufficient. I found in my office of twenty or so employees that a quarterly review consistently yielded at least one changed phone number or address.

A word of caution here: some employees may feel uncomfortable knowing their home address and phone numbers are being shared beyond those in the firm's management on a "need to know" basis. Employees may be reluctant to provide updates when they realize their contact information is being shared with the entire team. Explaining the purpose of the team and the need for contact information may help alleviate those fears. For those employees who continue to be reluctant, you might ask them what steps the firm can take to allay their fears. Assure

them that the information will only be used for contacting them during a firm emergency.

A Change in the Areas of Your Firm's Practice

This probably would not register as one of the top reasons to re-evaluate your disaster plans, so let me quickly make the case for it. Think about this: a firm transitioning from a commercial litigation practice to one that includes family law disputes inherently changes the types of people sitting in the firm's reception area. A waiting area previously occupied by business owners could now be filled with individuals going through divorce or child custody disputes. Although commercial litigation is not without emotion, family law matters are far more likely to be emotionally charged. Likewise, firms electing to branch into probate disputes might face risks akin to those moving into family law practice.

In addition to this possible change in clientele, switching your firm's area of practice could result in new (sometimes hazardous) materials entering the office. I've seen clients bring a number of interesting things into a law office for safekeeping or in response to discovery requests in family law matters, including firearms, electronic bug detection equipment, and surveillance videos of persons in compromising situations, just to name a few. Whenever such items are being brought into a firm, one's attention should perk up.

Similarly, firms beginning to work in the area of intellectual property or personal injury might want to make sure they do not inadvertently become custodians of dangerous materials. Lawyers are often tasked with securing evidence for a client; this evidence might be something quite hazardous to those working around it. Firms experienced in these practice areas generally know when it's acceptable to keep something in their office and when to ask for assistance in determining its risk. Let's face it: you don't want to be the lawyer who unwittingly stored volatile materials in the office supply closet as part of your client's case, only to have the community read all about it when your office is destroyed by fire as a result.

Testing the Plan

Some entrepreneurs have made a small fortune selling fitness formulas advertised as being able to give buyers the perfect beach body without the workout regimen they'd just as soon skip. "Just taking this healthy supplement with every meal gave me a killer body," the young, bikini-clad spokesperson claims. "And best of all, I didn't have to go to the gym to do it!"

These late night infomercials, while entertaining, mislead us into believing there's a shortcut to getting an awesome physique. Similarly, simply getting your plan together will no more get you ready for a disaster than taking some pills will make you look like a Victoria's Secret model. To truly be prepared for disasters, you have to exercise your plans just like a star athlete regularly exercises his or her body.

Testing the plans with disaster exercises need not be laborious. Below, I outline some options for you to consider in conducting exercises.

Table-Top Exercises

By far the most common and least expensive way to test your plan, table-top exercises can teach you a lot about your level of preparedness in a short amount of time. As the name implies, a table-top exercise entails sitting around a table in your office (or, for the more social-minded, a table at a local watering hole) and talking your way through a set disaster.

For example, let's assume that we're going to do a table-top exercise for an extended power outage at the office. The team members would get out their laptops or folders containing their plans and references and start talking through what they would do. One person might say, "I would be the one to contact the employees and tell them not to come to work that day." Another might add, "If you do that, shouldn't you also tell them when to expect to come back to work? And you might want to be prepared to answer questions about whether they will get paid while they are off work."

These ancillary discussions as you walk through the plan will help you find the weaknesses in it, and it's better to make these discoveries in the comfort of your conference room or during happy hour than when the office is dark and your clients and employees are wondering where you are.

To help you get started, I've included some sample table-top exercises in this book, as Appendix C. When creating scenarios on your own, keep in mind that you are only limited by your imagination. Be creative!

E-mail Exercises

During my stint as a volunteer firefighter, our chief loved to keep us on our toes by e-mailing the entire department a series of questions on various procedures and useful facts. He would ask us questions about certain hazardous materials procedures, the psi friction loss for a given length and diameter of hose, and how to assess a medical patient for treatment. Those who responded quickly and accurately often got a prize (usually bragging rights), and we all got a quick continuing education course in the process.

You can do the same thing in your office. E-mail your team sometime and ask them questions like:

- Where is the electrical breaker box for our office?
- What is the property manager's phone number?
- We have a shop vac stored at which employee's house?
- How often are our servers backed up? Where is our server located?
- Suppose a tornado warning has been issued for our area. What's our first order of business?
- Our office has been closed due to a plumbing disaster that has damaged our files. Identify where our alternative work locations are.

- The bank where we make our daily deposits was robbed earlier today and is surrounded by crime scene tape. Where is the closest alternative branch we can use to make our deposit?

Like our chief, you can make a game out of this, offering rewards and recognition to those who answer quickly and correctly.

This type of exercise does two things. First, it helps educate the team on the nuances of the plan in a fun and interactive way (especially if donuts or an hour off from work are riding on participants' preparedness). But more importantly, if done randomly, it gets your team regularly thinking about the plan and playing the "what if" game. Getting your team into that mindset will yield great dividends should the unfortunate occur.

The "Don't Try This at Home" Drill

We are often reluctant to test our equipment's abilities, either because we're afraid that it won't perform as it should or because we fear we might damage it in the process. Rather than fearing what might happen during a test, we should embrace the opportunity to learn whether the equipment will work as designed, postdisaster.

For your plan to work, you should be doing, on a regular basis, some things that may seem a bit perilous. And by that, I mean that you should consider:

- Powering down your server and restarting it from time to time. I've had people tell me they would *never* try this, because they feared that it wouldn't restart or that it would create havoc in their network. That is precisely why you *should* do it—if there's a problem on the restart, it's better to know now than immediately after a disaster.
- Firing up a generator you plan to use in a power outage. Large capacity generators have "exerciser" functions; about once a week, automatically start and run this function of your generator for several minutes to ensure that it stays in good working order.

- Attempting to access a file you backed up on an external hard drive. (True story: two days before I wrote this section of this book, I tried accessing a file on the external hard drive I use for backup on my home computer. Guess what? Despite reading the user's manual several times, I couldn't get it to work. That's something you want to know now, rather than later.)
- If you own your own building, turning off the gas and water to it. You may wish to call the gas company before you try this, as they may have certain safety precautions they want you to follow before you turn it back on. (I can tell you from personal experience that it's no fun trying to figure out how to do this at your home at 6:00 A.M. in February when it's twelve degrees outside. It's even less fun when the plumber tells you that the above-ground valve for your yard's irrigation system that burst from the cold weather—hence the need to turn the water off—will set you back $450. On a side note, it will make you a big believer in xeriscaping.)

You get the idea. Look through your plan and identify things that require you to use equipment or a system, and then test whether those things will actually do what they are supposed to do during an emergency.

Full-Scale Exercise

Some time ago, I was asked to draw up plans for a full-scale disaster exercise for my company's regional office. I'm happy to say that on game day we had—

- a fire engine and crew;
- a SWAT team, in their SWAT regalia and with their SWAT toys and mobile command trailer;
- employee volunteers on the scene—some with realistic-looking injuries, some acting as protestors, and some just being annoying;
- an EMS unit; and, as a cherry on top,
- a med-evac helicopter, which landed in the parking lot.

Know the best part about it? *It didn't cost us a dime.*

Most firms won't need a SWAT team or a helicopter as part of their full-scale exercise. (We didn't either, but it was a tremendous amount of fun.) If you do elect to call on your local first responder community, know that they really enjoy and appreciate the opportunity to help you out; they will likely not charge you anything, since you're already paying taxes. In addition, you are building a relationship that can really pay off in the future. I highly recommend involving such persons to some extent in your exercise. They are a treasure trove of knowledge and skill, and they can help you make huge strides towards your preparedness goals.

You will, however, need a few resources to make a mock disaster work well. These include:

- An exercise coordinator to run the drill. This person should *not* be on the disaster team. You want your entire disaster team learning from the exercise.
- An observer to take notes and share observations of the drill.
- A good scenario, with twists and turns that can be implemented during the course of the exercise. You want to create a sense of chaos early on, put some stress on your team's decision makers, and really force them to make decisions.
- A concise message to your employees about what you're doing and why you are doing it. Note that some employees may find a full-scale scenario rather stressful; make sure that you give those employees the resources they need to cope.
- A message to your office neighbors that you are conducting a drill on a given day and that they should let you know if they have questions or concerns.

Full-scale exercises will let you test multiple functions of your plan as well as train your staff, all at the same time. Keep that in mind when calculating the loss of productivity of your firm during the time spent in training.

Updating and exercising your plans do require a commitment of time and resources. But the result is a firm infinitely more prepared for a problem than one that simply files and forgets its disaster plan.

Chapter 9

Using Insurance as a Preparedness Tool

I'm an insurance guy. Having done insurance defense work and in-house counsel work for insurance companies my entire career, I will probably spend more time on this subject than most people would. But I think that many authors who write on the subject spend little time on insurance because they don't understand how it works.

Insurance is simply about transferring risk. You pay a premium, and in return, someone else—in this case, the insurance company—agrees to bear the burden of loss. That being said, it is *absolutely critical* that you understand the basics of insurance, your insurance policy, and the claims process to maximize your ability to use insurance as a preparedness tool.

Many insurance lawyers assume that all lawyers understand the basics of an insurance policy. However, from my experience in giving presentations on this subject at various CLE seminars to noninsurance lawyers, I can assure you that that is not the case. Many lawyers who are experts in their own respective fields of practice are not versed in

the nuances of the insurance industry or insurance law. Given that, it's important that you understand the following facts and elements of insurance coverage.

Basic Components of an Insurance Policy

1. *The policy itself*. This document defines terms and sets out the rights and obligations of each party. It describes what events are covered and not covered by the policy. For example, flood damage is not covered under most insurance policies. (Other flood coverage can be purchased through many insurance agents; flood policies are usually underwritten by the Federal Emergency Management Agency). The policy also describes what property is covered and not covered for damages. In addition, the policy language discusses your duties after an incident.
2. *Endorsements and schedules.* Simply put, endorsements to the policy expand or contract coverage. For example, something may be excluded under an insurance policy. Many times, you can buy an endorsement to add that excluded coverage back to your policy. Conversely, you can add endorsements to your policy that reduce the amount of coverage you have. Generally speaking, adding these kinds of endorsements lowers your insurance premium.

   Insurance companies may attach schedules to the policy. Schedules are lists of specific pieces of property stating the amount for which they are insured. For example, if your firm owned a unique piece of property—such as a work of art—for which the value may exceed the total value of all office equipment, it may be listed on a schedule to provide additional coverage.

3. *Declarations page.* The declarations page, or "dec page," is what makes the policy unique to you, as the insurance company's customer. The dec page will identify the insured party, the limits of coverage, a list of endorsements that are part of the policy, and the full legal name of the insurance company issuing the policy.

ACV or RC? Deductibles?

There are two other concepts that are very important for people to understand about insurance policies. The first is the difference between *actual cash value* and *replacement costs*. In its simplest terms, actual cash value is the market price of a particular piece of property. Replacement costs, on the other hand, reflect the market price to replace that piece of property with a brand new version.

For example, take a common chair you might find in a conference room of a law firm. Suppose that chair is fifteen years old and is in good condition. The chair, despite its condition, has depreciated over time. So the actual cash value—what the chair would sell for if you sold it as is in an open marketplace—might be $50. However, to *replace* that chair for a brand new one, the firm might spend far more than $50.

Why does this matter? In the policy, the insurance company will describe whether it pays for damage to property based on an actual cash value (often referred to as "ACV") or on a replacement cost (referred to as "RC") basis. As you can imagine, coverage on an ACV basis usually means the customer pays a lower premium, while coverage on an RC basis generally requires more premium. Depending on the insurance company, and the type of property insured, often the difference in premium is minimal. You should *always* ask your insurance agent to *price the ACV and the RC coverage separately*, so that you can get a better picture of what each coverage provides and the added expense of securing payment on an RC basis.

Secondly, people need to have a good understanding of the concept of deductibles. As you can imagine, a deductible is simply a dollar amount or a percentage of loss the insurance company's customer agrees to cover on his or her own. For example, if a particular item is damaged and the insurance company is obligated to pay $1,000 for it, subject to a $300 deductible, the insurance company will write a check to the customer for $700—that's $1,000 minus the deductible.

Deductibles are important in the insurance industry, as they shift some of the risk of loss back onto the insured, thus giving the insured some reason to take care and mitigate risks. You can often save money on your insurance premiums by requesting a higher deductible.

There's no right or wrong deductible. That's a decision that you, as a business person, must decide. Would you rather pay higher premium for a lower deductible, or lower premium for a higher deductible? Your insurance agent will help you decide.

What Coverages Do You Really Need?

Coverage for Business Property

Like any other business, law firms have physical assets needing insurance coverage. When you talk to your insurance agent, you should ask the following questions:

1. *What perils will the policy cover?* "Perils" are the various bad things that might occur—such as fire, wind damage, and theft, just to name a few. Insurance companies will provide coverage for perils in one of two ways. One way is to provide a "named peril" policy. Such a policy lists the perils for which it provides coverage. If a peril that affects your property is not on the list, then there's no coverage for your property under the policy for that peril. On the other hand, some companies

provide a "peril not excluded" policy—sometimes called an "all risk" policy. In this situation, the insurance company states what perils it does *not* cover. Any peril not on the list is, by default, covered. As you can see, the "peril not excluded" policy provides a wide range of coverages, simply because any peril not specifically excluded will be covered.

2. *Does my policy provide payment on an ACV basis or RC basis?* As discussed above, you should always ask this of your insurance agent. Some policies provide some coverages on an ACV basis and others on an RC basis. You will need to fully understand these when purchasing your insurance coverage.

3. *Does my policy cover my computer and equipment related to my computer?* Given the expense and complexity, many insurance companies have taken to writing special coverages for computer issues. For example, while the policy may provide coverage to replace your computer, this does not necessarily mean that it will provide coverage to recover the data that was stored on it. You will need to make sure you have a good understanding of this coverage when you buy the policy, as data restoration services can be quite costly.

4. *Does my policy cover property away from the premises?* If your firm owns a laptop and the laptop is stolen while it is away from the physical office—for instance, when one of the firm's attorneys takes it home or to a courthouse—will it be covered? Most policies provide some coverage for property away from the premises; however, you will need to confirm that with your insurance agent.

5. *With respect to damage to the office building, does my insurance policy provide for changes to building ordinances or laws?* Usually available by endorsement, this coverage provides for losses that may result from enforcement of building codes regulating the repair of insured damages to a building. In some instances, laws or ordinances prevent a building from being restored exactly as it was before it was damaged. The building code may require, in-

stead, that upgraded material be used or additional safety features be included as the building is repaired. As you can imagine, bringing a building up to code after a disaster may add additional expenses. You will need to decide whether you want to have that covered under your policy.

Coverage for Nonprofessional Torts

While a malpractice suit can bring damages both financially and to the reputation of a firm, such discussions are outside the scope of this book. However, it's important to remember that not all acts of negligence by a lawyer or law firm involve malpractice.

For example, suppose a client comes into your office and, while walking down the hall, slips and falls. Does your firm's liability policy provide coverage for that? Most basic commercial liability policies (often referred to in the insurance industry as commercial general liability or "CGL" policies) would provide coverage in such situations.

Let's look at another example. Your firm employs a number of "runners" who take documents to the courthouse for filing, deliver things to other law firms, and pick up supplies at local office supply stores. If one of your firm's runners is involved in an automobile accident while in the course and scope of employment with your law firm, is that covered by your firm's general liability policy? Many times, general liability policies for businesses do not provide coverage for automobile accidents. You will want to make sure that your policy provides you with additional coverage for this situation.

What about libel and slander? Given the nature of what lawyers do, it's conceivable that someone, upset with a lawyer, might claim that the lawyer committed libel or slander when discussing something that the person may or may not have done. Most insurance companies sell a special endorsement for libel and slander coverage; these endorsements are relatively inexpensive and add a large amount of coverage for these situations.

Business Interruption Coverage

If you learn one thing from this book—and only one thing—let it be this: *Make sure you have business interruption coverage on your insurance policy.* I cannot stress this enough. Business interruption coverage, while not expensive, provides great benefits for a relatively small premium.

As the name implies, business interruption coverage pays you money for lost profits, for salaries of your employees, and for the various ongoing expenses of keeping your firm up and going. Think about it: If your law firm was offline for six to eight months, with only a trickle of receivables coming in the door, how would you afford to make mortgage payments on your office? Or pay your staff? Or even pay yourself? That's where business interruption insurance comes in.

Within the scope of business interruption coverage comes utility interruption coverage. This coverage pays for loss of income caused by the necessary suspension of business due to interruption of water, natural gas, or electrical services to the insured's premises. The failure of service does not have to occur on the premises but must be caused by the specified peril.

For example, two blocks away from your office, a fire takes out an electrical substation, cutting off electricity to your office. As a result, your office can't function for several days. Under business interruption coverage, assuming you and your insurance agent have procured the right coverages, your firm would be entitled to make a claim under the policy, subject to its terms and conditions, for the loss of income due to the utility interruption—even though the interruption didn't happen on your premises.

Insurance isn't the most exciting topic. But it remains a very necessary one. Making sure you have the right kinds and amounts of coverage should be one of your "must dos" on your preparedness task lists. A good insurance agent can be invaluable in helping you make those decisions.

Chapter 10

Things That Will Make Your Personal Life a Lot Easier

In the preceding chapters, I've spent much time discussing how to protect your business from disaster. While preparing for disaster in your personal life may seem a bit outside the scope of this book, let me explain why it isn't.

First, knowing that your family has the basic supplies to help them weather the storm will make you more productive at work. Knowing that you have sufficient food, water, and medicine on hand to protect your family means that you have one less thing to worry about.

Next, many of the items that you would use on a personal level will help your business to recover as well. Your employees, just like you, will have needs after a disaster. Your ability to meet some of their personal needs will engender goodwill and increase their desire to help the firm get up and running again.

Finally—and I realize that many people don't see it this way, but some of you will—collecting preparedness toys is just plain fun.

Having said all that, I'd like to share with you a very basic list of things you might consider purchasing and keeping available that will improve the quality of your personal life during and after a disaster.

Water Purification

In the wake of Hurricane Andrew, I boiled water using my gas stove for days, as my zip code was under a mandatory order to do so. Being able to have fresh drinking water without having to rely on relief agencies or my nearest store helped me tremendously.

I don't care how much insurance you have or how many procedures you have written down, if you don't have anything to drink, all of those other things are irrelevant. You need access to clean water.

There are a number of ways to get clean water. One item in my family's house that has worked well is the Berkey water filtration system, which comes in assorted sizes for multiple applications. Although these systems are not cheap—our model cost around $300—they do provide some of the finest water filtration available. Further, they do not need chemicals or electricity to work. Just pour the unsafe water in the top chamber, and within an hour or so the filters will do the rest. Regardless of what water purification method you use, make sure you keep the supplies on hand to make it work.

Food

After a large-scale disaster cuts off the electricity, most people will quickly eat up all of their perishable goods. This means that pretty soon nonperishables are all that's left. I learned very quickly after Hurricane Andrew that Spam fried in a skillet was not the way to go.

Think about keeping nonperishable foods on hand for emergency purposes. By "nonperishable," I mean things that store well, such as canned goods, as well as basic staples like beans, rice, and grains, which require no refrigeration. Powdered drink mixes will also help break the monotony of drinking water.

Communications

I keep a wide assortment of radios and battery-powered televisions. Having said that, nothing beats a small, handheld transistor radio with AM and FM band functions. In an emergency, a battery-powered transistor radio with these capabilities will provide you with an ample amount of news and information, especially on the AM band.

Of course, most people now carry cell phones, many of which allow Internet connectivity. Cell phones are thus also useful communication devices during disasters, as they are battery-powered and can allow you to both check on your loved ones and access news through the Internet. Moreover, the Federal Communications Commission plans to roll-out a new emergency alert system nationwide in 2012 that will make cell phones increasingly useful during disasters. The new system will send text messages directly to cell phones of consumers in specific, targeted geographic locations whenever that area is faced with a major threat such as a natural disaster or national security concern.[1]

Chainsaw

Let me say it before someone else does: chainsaws are dangerous. You can seriously hurt yourself with them. After Hurricane Andrew, hospitals in the Miami area saw a huge spike in visits to the emergency room due to chainsaw accidents. Many of these accidents were caused by first-time chainsaw owners trying to remove debris from their yards.

A chainsaw can make a world of difference in your efforts to clean up your property. It may also help you to remove items blocking your way to and from work. While not for everyone, for those willing to spend some time and effort in learning how to use one safely and effectively, a chainsaw can dramatically help your recovery.

1. Edward Wyatt, "Emergency Alert System Expected for Cellphones," *New York Times*, May 10, 2011.

Cash

When we lose power, or when power remains on but people begin to panic, you can bet your local ATM will either (a) not function or (b) be completely drained of money in short order. Always keep a decent amount of cash on hand in a safe location in your house for that very scenario. In addition, it is a good idea to choose a bank with a regional or national presence. That way, should your local branches be affected by a disaster, branches in other towns will still be open for business. The careful selection of a bank is thus important for a firm to consider, as well as individuals.

Batteries

One of the things I like to do when a storm approaches the Texas coast and threatens the Austin area is go to my local home improvement stores and grocery stores to see what people are buying. Not too surprisingly, people stock up on water, canned food, and batteries. Batteries are useful for a number of things. You don't want to be fishing in your battery drawer or taking batteries out of your kids' toys when a real emergency comes. Further, having batteries available for neighbors and coworkers will engender goodwill. So don't forget to stock up on batteries, and when you do, make sure you have them in the correct sizes for your various devices.

First-Aid Kit

No one likes to think about being injured. But in a time of crisis, we can expect certain types of injuries to go up (remember the chainsaw we discussed above), and in some situations, hospitals may be closed or completely overwhelmed. If you keep a stockpile of basic first-aid supplies, you will be able to tend to minor wounds without a trip to the ER. Further, any prescription medications taken on a regular basis, especially those necessary for life, such as insulin, should be kept in sufficient quantity to ensure that enough is on hand at any given time.

Power Inverters

An inverter converts battery power, usually measured in direct current (DC), into alternating current (AC). The things you plug into electrical sockets, such as computers, fans, and power equipment, all run on AC. A power inverter will allow you to take your battery out of your car or truck and, with some limitations, run basic appliances and equipment from it. You will need to research carefully what size inverter you need, being mindful that when you draw power out of your battery, you will need to recharge it somehow. The recharge may be accomplished by putting it back into your car and letting the alternator charge it while you drive—again, your battery must have enough power to actually start the car in that situation—or by a solar-powered battery charger, which can be purchased from a number of sources.

Personal Hygiene Items

In a disaster that affects electricity and water service to your house, keeping yourself clean may be challenging. Think about how you would bathe, brush your teeth, or shave in an emergency. Having lived in Miami for seventeen days in the summertime without electricity, I can assure you that being able to take a shower—even a cold one—and getting clean greatly improves your morale.

Entertainment

When I think of my stepdaughter and of the things she and her friends use to amuse themselves, one thing is common: electricity. It may be electricity from an electrical socket or from something that is battery-powered, but make no mistake—if the power is off, she's not going to be happy. Entertainment not requiring electricity, such as books, board games, decks of cards, art supplies, and basic sporting goods equipment, will go a long way toward keeping kids (and adults) entertained while waiting for the utilities to be restored.

Self-Defense Equipment

I'm not going to spend a lot of time on this, because this topic can be quite controversial. But experience tells us—from the hurricanes we've had over the last twenty years, to the riots in Los Angeles in 1992, to the Northridge Earthquake in 1994—that police cannot be everywhere all the time. You will need to take steps to protect yourself and your family from those individuals who wish to take what's yours, inflict harm on you, or both. At the end of the day, you must decide what course of action to take. I would encourage you to think *now* about what you would do *then*.

Resources Available for Personal Preparedness

A number of books and Web sites are devoted to this subject. A really good starting point is a book published by FEMA entitled *Are You Ready? An In-Depth Guide to Citizen Preparedness*.[2] If you follow the instructions and recommendations of that book, you will be better prepared than the vast majority of Americans.

2. *Are You Ready? An In-Depth Guide to Citizen Preparedness*. (Washington, DC: Federal Emergency Management Agency, 2004).

Chapter 11

A Journey Begins with a Single Step

Musician Steve Earle released an album in 1991 entitled *Shut Up and Die Like an Aviator*. At one point between tracks, Earle states, "Just because you ain't paranoid don't mean they ain't out to get you."[1]

The goal here is not to make you paranoid by any stretch. It's simply to make you aware of the possible problems that might affect your business and life. Not thinking about the things that could go wrong and not planning for them won't make them nonissues. Those perils will still be out there, like it or not. Rather than ignore what might happen, I would encourage you to embrace it, prepare for it, and then relax, knowing you have a solid plan in place to handle whatever might come up.

Too often, we get lulled into a false sense of security. We go for years—if not decades—without our building catching on fire or a tornado hitting the office. It's human nature to fall into a routine and

1. Steve Earle and the Dukes. *Shut Up and Die Like an Aviator*. MCA B000002OH1, compact disc. Originally released in 1991.

become complacent. Yet when things do go wrong, they can do so very quickly and very badly.

Just a small amount of vigilance and preparedness can keep your business up and running while others flounder. An hour with your insurance agent ensuring that you have the right coverages could make the difference between having tuition money for your college-age kids and having to tell them you're a little short due to the disaster at the office. A quarterly lunch meeting with your staff to review the disaster plans for the office could mean the difference between everyone knowing what to do in a workplace violence situation and having someone tragically harmed in the event. A weather radio may make the difference between safely staying at the office a little longer and inadvertently driving home into a dangerous storm.

As the ethics rules and the standards of care evolve, don't expect the need to be prepared to diminish. Technology continues to provide better ways to store large quantities of data in small and inexpensive ways. Meanwhile, threats to that data continue to grow and evolve. Simply throwing the files in the filing cabinet before you leave the office for the day may not be sufficient in the future; we may be required to take additional steps to comply with various legal and ethical obligations.

If you're feeling a bit overwhelmed at the prospect of developing and maintaining a disaster plan, rest easy. Remember there's only one way to eat an elephant—one bite at a time. Start with the basics. Put yourself on a realistic schedule in your efforts to get the office prepared. Discuss your efforts with others in your local bar associations and networks. Recruit others in your organization to help. When you have questions, reach out to the experts, or feel free to call me. In the end, don't go it alone if you can avoid it.

Finally, realize that this is an ongoing process. Your business will change over time. Employees will come and go. Your office may move across town. Your use of technology will change as well. Keep on top of your plans, keep your disaster teams sharp, and make changes when needed.

Good luck—and get prepared!

Appendix A

Additional Emergency Gear That a Business Should Keep on Hand

- Large trash bags in which to place computer equipment and other water-sensitive items, and to have available for clean up
- Basic tool kit
- "Shop vac" or other heavy-duty vacuum cleaner with water-removal capability
- Fans of various sizes to help ventilate the office or to keep cool working in an alternative work site
- Extension cords to run electrical equipment after a disaster
- Battery-powered transistor radio for news and information during power outages
- Power strips to provide surge protection for computers when working at alternative work sites
- Extra batteries to run the various flashlights and radios
- Snacks, including powdered drink mixes

- Generator to provide power for basic electrical needs in case of a power outage
- Uninterrupted Power Supply to provide extra power during a power outage so computer users can save current data and power down safely
- External memory devices, such as hard drives or flash drives, to back up firm data or to secure disaster plans
- Basic office supplies (pens, legal pads, folders, etc.) in a water-tight container reserved for use solely in a disaster situation

Appendix B

Most Common Threats to Your Office

Infrastructure Issues

At Your Office:

- Fire in your office
- Fire in a neighboring office, making your office unusable
- Plumbing failure at your office, causing damage
- Plumbing failure at your office, not causing damage but making office unusable
- Plumbing failure at a neighboring office, making your office unusable
- Electrical failure limited to your office
- Hazardous materials incident in your office

- Hazardous materials incident in a neighboring office, making your office unusable
- Heating, ventilating, or air conditioning failure at your office, making your office unusable or uncomfortable

In the Area Around Your Office:

- Area electrical black-out, affecting offices, local businesses, and traffic control signals near office
- Area water outage, making all businesses around office unusable
- Hazardous materials incident nearby, causing local officials to limit access to your office

Weather/Natural Disaster Issues

Directly Affecting Your Office:

- Storms damage your office, causing the roof to leak and water and wind to be blown in through broken windows
- Possibility of injuries due to flying debris
- Power outage in office, making egress after storm difficult
- Flooding from heavy rains causing significant water damage to your office
- Brown-outs or black-outs at your office due to increased electrical demand during hot summer months
- Wildfires brought on by drought conditions, affecting offices near wooded or brushy areas

Indirectly Affecting Your Office:

- Strong storms knock down trees, knock out power, or flood roads, affecting your ability to get to your office

Man-Made Issues

Intentional Acts:

- Workplace violence at or near your office
- Criminal acts near your office but not associated with the workplace

Appendix C

Suggested Table-Top Exercises

Note that the exercise facilitators may choose to give the facts of the scenarios to the team incrementally to allow time to discuss and think through each step after each set of facts is provided.

Exercise 1: Plumbing Failure in the Office
Level of difficulty: basic

Scenario

On Tuesday morning, your staff contacts you to report that a plumbing line in the ceiling above your file room failed overnight, causing extensive water damage to a number of files and office equipment, such as the postage machine and one computer. The water has seeped through the carpeting to roughly a third of the office, which "squishes" when you walk on it.

In addition, in the offices affected with water damage, several of the attorneys' bankers boxes, stored on the floor, have absorbed a fair

amount of water, further damaging their contents. Some of these attorneys have active trial practices, and the documents in some of those boxes were to be used as evidence at a trial starting next week.

The office is already beginning to smell. Fortunately, the plumbing line that failed contained potable water; thus we are not dealing with a situation involving raw sewage. However, the carpet is fairly old, hasn't been professionally cleaned in several years, and the smell of the dirty carpet and wet cardboard is becoming stronger by the minute.

Questions:

- What are the first three things that you do?
- What steps do you take to mitigate the property damage?
- How do you propose reconstructing the evidence that will be needed at trial? Do you seek a continuance? If so, how do you document the hardship that has affected your office?
- Does your insurance cover broken water pipes and the damage they cause?
- Who do you call to start the repair process? Must you call the landlord? If the landlord is unresponsive, do you call someone yourself to begin the repairs? If so, who?
- Some of your employees begin to complain that the smell is too much for them. Further, some claim that they are hypersensitive to mold and allergens, which they say have been stirred up by the leak. How do you address these employee issues?
- At what point do you decide to move to an alternative work site?

Exercise 2: Tornado Warning
Level of difficulty: moderate

Scenario

At lunch time, you get word that the National Weather Service has issued a tornado watch for your area until 7:00 P.M. Many of your employees are out of the office and won't return until 1:00 P.M. or so. You check the radar and see storms forming about 100 miles away, moving toward your area.

At 3:00 P.M., your staff advises you that the sky is getting very dark and the wind is picking up. The radar shows that the storms have grown in size and have moved much closer to your office.

Around 4:00 P.M., the National Weather Service issues a tornado warning for your county. They expect a storm capable of producing a tornado, strong winds, and hail one inch in diameter to pass near your office by 4:20 P.M.

One of your employees, Samantha, has a paralyzing fear of severe storms. One of her coworkers tells you she is "starting to freak out big time" and cannot perform her job functions. She begins crying as she cannot get her kids to answer her phone calls.

At 4:15 P.M., the power goes out. You can now clearly hear the winds buffeting your building, followed by the sound of glass shattering and people screaming. You yell out for people to take cover. People continue to yell, some of whom you believe have been injured.

At 4:20 P.M., the winds start to subside. You notice the temperature in the building has dropped several degrees. You walk around as best you can in the darkened office, hearing several people moaning and crying. The glass has been knocked out of several windows, allowing colder air into the office. You try to find out who is still in the office and who is missing. Someone tells you that your firm's court runner and one attorney were seen leaving the office just before 4:15 P.M.

From a conference room, you hear voices that you don't recognize. As you make your way to the conference room, you realize that one of your associates had been taking a deposition of a witness when the storm hit. The court reporter, opposing counsel, and witness seem a bit disoriented in the dark and in an unfamiliar office.

Meanwhile, a staff member reports that Samantha is nowhere to be found. Further, it appears that two employees have suffered minor injuries when they tried to take cover from the storm in the dark. As you look out the window into the parking lot, you notice that several employees' cars have been severely damaged by debris, making them undriveable.

Questions:

- What actions, if any, do you take when you learn of the tornado watch?
- What actions, if any, do you take when the staff reports the weather conditions at 3:00 P.M.?
- What actions, if any, do you take at 4:00 P.M. when the tornado warning is issued?
- What do you do about Samantha when you hear that she is not handling the prospect of the storm well?
- Once the storm subsides, what do you need to accomplish in the first ten minutes?
- At 4:45 P.M., Samantha still has not been found. What steps do you take regarding her situation?
- For those employees with damaged cars, how do you get them home?
- Your office will likely be without power for at least a day and without some windows for a few days. What steps do you take for alternative work arrangements?

Exercise 3: Workplace Violence
Level of difficulty: difficult

Note that some people may find this exercise objectionable. Given the risk of workplace violence, employers should not shy away from dealing with this difficult subject. But those who find this scenario too distasteful should change the fact pattern to make it more palatable. As your team's sophistication and experience level grows, however, you will need to challenge them with more difficult situations like this.

Scenario

Your three-lawyer firm has a diverse practice, which includes criminal defense, family law, personal injury, and probate work. On any given day, the firm has a large number of nonemployees coming in and out of the office, including clients, witnesses, and vendors. These visitors may be in the office to meet with staff, participate in depositions, and sign documents. Your firm employs six nonattorneys in various roles—receptionist, secretaries, paralegals, and file clerks.

On Monday, your paralegal, Erin, calls in to say she is running late because she isn't feeling well. When she does arrive, she appears rather flustered and upset. She confides in a coworker that her husband, David, left the home in the middle of the night after an extended argument. She believes that David is having an affair and had confronted him about it last night. Asked if she is okay, Erin responds, "I am okay, but I am really scared. David has a temper and can be really violent sometimes."

Two days go by rather normally. On Thursday afternoon, a woman calls the main firm phone number and asks if Erin is at work that day. The receptionist advises that she is. The caller says, "Thanks. I have a delivery for her and wanted to make sure she's there to receive it." Given the nature of the firm's practice, deliveries are common, although it is a bit unusual to call to confirm that the recipient will be at the office.

Around 3:30 P.M., a female visitor enters the firm's reception area, carrying a banker's box. The visitor identifies herself as "Callie," who has a delivery for Erin from "some lawyers in town." The receptionist

calls Erin to come to the lobby to meet Callie.

When Erin enters and introduces herself, Callie says, "Hi, Erin. I have something for you." Callie opens the box and pulls out a handgun. "David loves me now, and if I can't have him, neither can you!" With that, Callie fires three shots into Erin's chest. The receptionist screams and runs down the hall of the office.

Scott, a young lawyer in the firm, steps into the reception area to see what the commotion is about. He sees Erin lying there with Callie standing over her. Callie looks up and makes eye contact with Scott. "Are you a lawyer?" she asks.

Scott, not sure what the correct answer to the question is, says, "Look, we need to relax here. I understand you're upset, but . . ."

Callie cuts him off and points the gun at him. "Typical lawyer. Can't answer a simple question."

Scott immediately dives back into the hallway for concealment. Unbeknownst to both of them, another lawyer in the office, Stan, has come into the reception area from behind Callie. He takes advantage of Callie's fixation on Scott and tackles her. In the ensuing scrum, the gun discharges again, striking Stan in the leg. He and Scott are able to subdue Callie until the police arrive five minutes later.

First responders arrive. Paramedics take Erin off on a stretcher after completing emergency aid. Stan is also taken to the hospital, although his injuries are much less severe. Callie is taken into custody. The police department declares your entire office a crime scene and ushers everyone out of the office.

Meanwhile, the firm's employees remain in shock. Some break down into uncontrollable weeping. Some are angry. All of you are in the lobby trying to make sense of the situation.

As you try to console the employees, a TV reporter and camera crew come into the lobby. They recognize you as an attorney in the firm, due to your profile picture on the firm's Web site. The reporter starts peppering you with questions about what happened and what your firm might have done to prevent something like this from happening.

Questions:

- At what point would you want to know about Erin's and David's problems?
- Assume for a moment that Erin told you about her situation on Tuesday. What would you have done at that point? Would you have told the receptionist to be extra vigilant? If so, do you run the risk of upsetting Erin for sharing embarrassing details of her personal life with others in the firm?
- Is the call inquiring whether Erin is there for a delivery something that should alert the firm?
- Should Scott and Stan have tried to engage Callie or should they have left the building as quickly as possible, helping their coworkers do the same?
- Since the police now have control of your office space for its investigation, how do you conduct your business? How do you get those employees home who left their purses and car keys in the office?
- Is the building lobby the best place to meet after a disaster? Where will your firm meet to take roll call and share information?
- An event like this will certainly take a toll on your firm's morale. Many employees, once back to work, will find it very difficult to focus. Some may not return to work at all. In addition, some clients may feel trepidation about contacting or visiting the firm's office. What do you do to address these issues?

Appendix D

Sample Disaster Plan

Last Update: _____

DISASTER PREPAREDNESS AND BUSINESS RECOVERY PLAN

Introduction

The following plan is designed to—

- provide a framework for a base-line level of disaster preparedness for our firm and
- give the firm options in the event of a disaster affecting the building and/or our firm's ability to function.

Incident Response team members: John Doe, Jane Doe, Jack Doe

Business Continuity team members: Sarah Doe, Sam Doe

To give our firm the necessary flexibility in times of disaster, we should strive to—

- have all attorneys take their laptops home every night;
- have at least two paralegals take their laptops home every night (specific paralegals can be designated to do this every night or the responsibility can be rotated on a daily or weekly basis); and
- make sure that all files ready to be returned to the file cabinets are in fact returned every night and that the cabinet drawers are closed to prevent potential water, wind, or fire damage to those files.

Before a Severe Weather Event

Before leaving the office in anticipation of severe weather or some other disruption, we should—

- record an outgoing voicemail message that includes a cell phone number;
- take laptops home;
- take work home to perform should the office not be open the next day; and
- turn on our e-mail out-of-office message to alert others that staff is not in the building due to inclement weather.

Possible Disaster Scenarios and Our Response

After a disaster, the incident response and business continuity team members will contact managing partner Becky Barrister or her backup, partner Barry Backup, as soon as possible to assess team member availability and to begin assigning recovery tasks. The team may elect to have a conference call immediately after the disaster to strategize and formulate the team's response.

Here are two potential disasters and how we would react to them:

Scenario I: Substantial or Total Loss of the Office

In the event the office is lost due to fire, storm, or other disaster, our firm could potentially relocate to the Austin office of Large Law Firm. It is located at 412 Perfection Drive in Suite 310. The phone number is 512-555-1212. The business continuity team will attempt to contact fellow staff members to let them know where we will be meeting.

IMPORTANT: Do not report to Large Law Firm until arrangements have been made to use their space.

If Large Law Firm's office becomes our temporary home, we will need to—

1. work out a schedule for employees to come to the office, since Large Law Firm's office may not accommodate everyone in our office;
2. notify the court clerk's office and opposing counsel of our whereabouts;
3. work out a schedule for someone to remain at our office to accept mail and coordinate access for repair teams;
4. consider posting a sign disclosing "hours of service" and our alternate office location;
5. file for continuances and create supporting affidavits, if necessary;
6. obtain the requisite office supplies Large Law Firm does not have;
7. inform clients of our new address and phone numbers;
8. determine procedure to recreate existing files, if necessary; and
9. continue to answer outstanding discovery.

Scenario II: Catastrophic Damage to Our Office and to Other Buildings in the Area

In this scenario, Large Law Firm has also been affected by the disaster and is not an option for our firm's temporary relocation. This presents an incredible logistic scenario. However, for the first week or two, we will follow this procedure:

1. Scott will set up a make-shift law office at his home. Scott's home phone number is 512-555-7894.
2. Scott will notify as many opposing counsel and clients as he can about an alternative telephone number—preferably a dedicated cell phone—and a new P.O. box.
3. Scott will also notify the local court clerk of our plan and whereabouts.
4. The attorneys will work out a schedule so that someone is available to regularly check the mail box and be available to take calls from clients. Suit papers and subpoenas will be faxed and/or scanned and e-mailed to the appropriate attorney for handling.
5. We will need to work out a schedule for the staff to rotate days they will spend at Scott's make-shift law office.
6. Scott will assign files to the attorneys and paralegals, which they will work on from their homes using laptops.

Solutions to Possible Problems

Communication

We will establish a telephone tree to quickly inform all employees about new office hours, locations, and other necessary information.

In the event that we all need to meet in person at a central location,

potential venues include—

- another law firm's offices or
- a mall or shopping center.

Should we have a catastrophic failure of the telephone system, we will use the telephone tree to develop plans for the recovery team to drive to everyone's home to inform them how the recovery plan will take shape. Provided we can access the building, we will also use a "message board" system for people to check in at the office to see when and where to report for work.

If need be, we can use professional copying services to fax documents to opposing counsel, courts, and clients.

Receiving Suit Papers and Subpoenas

After a disaster, we will need to have an attorney available to accept and review suit papers and subpoenas. The attorneys should work out a schedule to rotate that duty among themselves.

We will post a sign disclosing the "hours of service" and alternate service locations where papers will be accepted if full-time staffing is not available at any make-shift office.

Considerations for Initial Group Meeting

If the group must meet off-site to get organized, the business continuity team must accomplish several tasks. Suggested items to discuss include:

1. The physical and mental well-being of the group. Does anyone need basic items such as food or water? Have child-care obligations been met? Assisting with the most basic needs of the group will engender goodwill and will enable everyone to focus on business operations more quickly.
2. Personnel accountability. Have we heard from everyone? Is anyone missing? Do we need to go to someone's house to

check on a staff member?

3. Establishing a workflow and schedule for off-site operations. Some employees may not be able to travel very far. The business continuity team needs to evaluate who is able to help and who is not.
4. Establishing a method to accept suit papers and subpoenas. Generally, one of the attorneys should be at the office for this purpose, unless other arrangements have been made.
5. Whether office supplies need to be purchased. Depending on where we elect to house our operations, this may not be necessary.
6. Creating a team to work with office management and computer service technicians to get backed-up items burned to CD or in some other electronic format for our use.

Personal Protection

Each employee should consider keeping basic necessities in his or her desk or vehicle. These might include—

- prescription medications;
- basic toiletries; and
- high energy snacks.

Also, employees should discuss with their child-care providers and older children a contingency plan in the event that a disaster prevents us from picking up our kids from school or daycare.

Appendix E

Launch Code Card Templates

Multiple templates of launch code cards can be found on page 104. Photocopy the cards, fill in the missing contact information, and distribute them to members of your incident response/business continuity team. Alternatively, use the templates as a guide for creating launch code cards designed for your firm's specific plan or needs.

Insurance Agent: ____________	Call 911 if necessary
Neighboring Law Firm: ____________	Ensure employees are safe/complete PAR
Remediation Company: ____________	Contact insurance company
Court Reporting Firm: ____________	Notify absent employees
Rental Car Company: ____________	Take mitigation steps if possible
Computer Support: ____________	Advise firm leadership
Office Manager: ____________	Arrange to get employees home if needed
Managing Partner: ____________	Notify court reporters/courts of situation if needed
Accounting Firm: ____________	
Office Supplies: ____________	

Insurance Agent: ____________	Call 911 if necessary
Neighboring Law Firm: ____________	Ensure employees are safe/complete PAR
Remediation Company: ____________	Contact insurance company
Court Reporting Firm: ____________	Notify absent employees
Rental Car Company: ____________	Take mitigation steps if possible
Computer Support: ____________	Advise firm leadership
Office Manager: ____________	Arrange to get employees home if needed
Managing Partner: ____________	Notify court reporters/courts of situation if needed
Accounting Firm: ____________	
Office Supplies: ____________	

Insurance Agent: ____________	Call 911 if necessary
Neighboring Law Firm: ____________	Ensure employees are safe/complete PAR
Remediation Company: ____________	Contact insurance company
Court Reporting Firm: ____________	Notify absent employees
Rental Car Company: ____________	Take mitigation steps if possible
Computer Support: ____________	Advise firm leadership
Office Manager: ____________	Arrange to get employees home if needed
Managing Partner: ____________	Notify court reporters/courts of situation if needed
Accounting Firm: ____________	
Office Supplies: ____________	

Insurance Agent: ____________	Call 911 if necessary
Neighboring Law Firm: ____________	Ensure employees are safe/complete PAR
Remediation Company: ____________	Contact insurance company
Court Reporting Firm: ____________	Notify absent employees
Rental Car Company: ____________	Take mitigation steps if possible
Computer Support: ____________	Advise firm leadership
Office Manager: ____________	Arrange to get employees home if needed
Managing Partner: ____________	Notify court reporters/courts of situation if needed
Accounting Firm: ____________	
Office Supplies: ____________	

Digital Product Documentation

Bracing for Impact: A Practical Guide to Preparing for Disasters Digital Product 2011

The digital product version of *Bracing for Impact: A Practical Guide to Preparing for Disasters* contains the entire text of the printed book. If you have questions or problems with this product not covered in the documentation available via the URLs below, please contact TexasBarBooks at (800) 204-2222, ext. 1499, or e-mail **books@texasbar.com**.

Frequently Asked Questions

For answers to digital product licensing, download, installation, and usage questions, visit TexasBarBooks Digital Product FAQs online at **http://texasbarbooks.net/f-a-q/**.

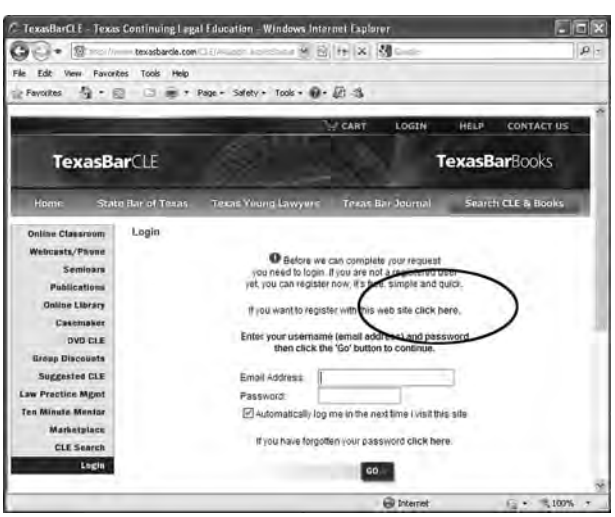
Downloading and Installing

Use of the digital product is subject to the terms of the license and limited warranty included in this documentation and on the digital product download Web pages. By downloading the digital product, you waive all refund privileges for this publication.

To download this book's complete digital product, follow the instructions on the following pages:

1. Type **http://www.texasbarcle.com/bracing-for-impact/** into your browser's address bar and press your keyboard's "Enter" key.

2. If you are not yet a registered user of TexasBarCLE's Web site, use the "click here" link to complete the quick, free registration. Otherwise, simply log in.



3. The initial download Web page should look like the one below.

See **http://texasbarbooks.net/download-tips/** for more download and installation tips.

Transfer: You may not transfer any copy of the material in the files or in the documentation to any other person or entity unless the transferee first accepts this agreement in writing and you transfer all copies, wherever located or installed, of the material and documentation, including the original provided with this agreement. You may not rent, loan, lease, sublicense, or otherwise make the material available for use by any person other than the permitted users except as provided in this paragraph.

Limited warranty and limited liability: THE STATE BAR MAKES NO WARRANTIES, EXPRESS OR IMPLIED, CONCERNING THE MATERIAL IN THESE FILES, THE DOCUMENTATION, OR THIS AGREEMENT. THE STATE BAR EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND OF FITNESS FOR A PARTICULAR PURPOSE. THE MATERIAL IN THE FILES AND IN THE DOCUMENTATION IS PROVIDED "AS IS."

THE STATE BAR SHALL NOT BE LIABLE FOR THE LEGAL SUFFICIENCY OR LEGAL ACCURACY OF ANY OF THE MATERIAL CONTAINED IN THESE FILES. NEITHER THE STATE BAR NOR ANY OF THE CONTRIBUTORS TO THE MATERIAL MAKES EITHER EXPRESS OR IMPLIED WARRANTIES WITH REGARD TO THE USE OR FREEDOM FROM ERROR OF THE MATERIAL. EACH USER IS SOLELY RESPONSIBLE FOR THE LEGAL EFFECT OF ANY USE OR MODIFICATION OF THE MATERIAL.

IN NO EVENT SHALL THE STATE BAR BE LIABLE FOR LOSS OF PROFITS OR FOR INDIRECT, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF THE STATE BAR HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES. THE STATE BAR'S AGGREGATE LIABILITY ARISING FROM OR RELATING TO THIS AGREEMENT OR THE MATERIAL IN THE FILES OR IN THE DOCUMENTATION IS LIMITED TO THE PURCHASE PRICE YOU PAID FOR THE LICENSED COPYRIGHTED PRODUCT. THIS AGREEMENT DEFINES YOUR SOLE REMEDY.

General provisions: This agreement contains the entire agreement between you and the State Bar concerning the license to use the material in the files. The waiver of any breach of any provision of this agreement does not waive any other breach of that or any other provision. If any provision is for any reason found to be unenforceable, all other provisions nonetheless remain enforceable.

LITIGATING ON THE CLOUDS

RONALD L. CHICHESTER, ESQ.
ron@txcomputerlaw.com

State Bar of Texas
PERFECTING YOUR PRACTICE 2010
November 19, 2010
Austin

CHAPTER 5.2

Litigating ~~Computing~~ on the Clouds

By Ronald L. Chichester, Esq.
ron@txcomputerlaw.com

January 8, 2010

Abstract

Although storing and manipulating data on remote servers via the Internet is not a new technology, it has recently been refashioned into a new service offering, generally referred to as "cloud computing." The pervasive use of cloud computing presents new challenges to lawyers and forensic examiners who are attempting to identify, collect, preserve, analyze and present electronically stored information ("ESI") that is not within the dominion of the data custodian. This paper presents identifies various issues related to cloud computing, such as benefits, security, e-discovery, forensics, service contracting and the like.

Keywords: Cloud Computing, Litigation, Electronic Discovery, Digital Forensics, Network Forensics, Internet Service Provider Contracting, Law Enforcement, Privacy, Social Networking

Table of Contents

Litigating on the Clouds

Things to Know When Your Data (or Your Client's Data) is Stored on the Internet

By Ronald L. Chichester[1]

Introduction

> "[O]ur social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the "cloud," on servers owned by internet service providers." *State v. Bellar,* 231 Or.App. 80, 217 P.3d 1094 (Sept. 30, 2009).

There are many benefits to cloud computing. Indeed, the benefits are so many that adoption of cloud services is crossing that tipping point where more adoption leads to yet more adoption. Moreover, certain applications, such as Google Wave,[2] take advantage of various network effects that traditional software applications can't match. Consequently, attorneys should know the perils and pitfalls of this not-so-new technology; not only for their own practice, but also for their client's wellbeing.

For this paper, I will adopt the convention of speaking about clients. However, law firms and attorneys must recognize that the issues presented herein apply to you and your firm. As attorneys, you may be involved in securities or malpractice litigation, and the warnings and issues presented in this paper are equally applicable to you.

What is cloud computing?

Cloud computing is the placing of data and/or a software application onto a (third-party) server that is accessible via a wide area network, such as the Internet.[3]

Essentially, the user interacts with their data and/or the software applications used to manipulate that data, typically via a web browser on any device capable of connecting to the World Wide Web of the Internet. Cloud computing will not completely supplant "normal" (PC-based) computing, at least initially. However, more and more services are being accessed online, and the trend is unmistakable – and unstoppable. Indeed, the trend has been likened to rural electrification in the early 20th Century, wherein power generation was centralized and electricity was distributed within a grid, not unlike the Internet.[4]

What are the benefits?

The benefits to consumers and businesses alike are apparent. The user does not have to download or install software onto their machine. Instead, the user simply employs the web browser(s) that come pre-installed with their network-capable device.[5] The customer need not purchase a powerful personal computer or the attendant software. The "heavy lifting" can be accomplished on the provider's server. The provider implements updates to the software in the background without affecting the user's experience. Infrastructure costs are reduced, and training costs are curtailed significantly. More importantly, the tie-ins traditionally imposed by linking office software to operating systems, such as Microsoft Office/Windows, is effectively broken, making cloud computing a particularly disruptive technology.

What are the problems?

Instead of buying software and (extra) hardware, the user has to rent space and/or bandwidth on a provider's server.[6]

Normally, however, the rental costs are far less than the cost of software and attendant hardware infrastructure – which is why cloud computing is so compelling. However, with the loss of infrastructure comes the loss of dominion (*i.e.,* both ownership and direct possession) over your data, possession being nine-tenths of the law. Loss of dominion can come in several forms.

First, the service provider may store your information in a proprietary format, making it difficult to "liberate" your data for backup, transfer, or production during discovery. Such tactics are common in the software industry (the proprietary format for Microsoft's Office documents being the most obvious example).

Second, the provider may assert ownership of the data by virtue of contract or Copyright. While facts are not copyrightable, the selection and arrangement of facts in a database may qualify for protection under the Copyright Act, and it is the provider that makes the selection and arrangement, typically as something other than a work-made-for-hire. In general, however, the federal copyright law does not protect databases, which is why service providers may be prompted to include specific data ownership terms in their contracts.

Third, the service provider can interrupt access to your data at any time. They have control over their servers, and can use that control to their advantage. Remember, you're "renting" space on their server. Failure to abide by their rules, or failure to pay the rent can result in termination of access, akin to eviction in real property law.

Finally, there is the issue of data security. For a detailed assessment of the pros and cons of cloud computing (with an eye toward security), see "Cloud Computing Risk Assessment" by the European Network and Information Security Agency ("ENISA"), which is a 125-page critique of available technologies and security issues.[7] ENISA concluded that:

> "the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective."[8]

Legal Implications of Cloud Computing

There are several legal implications in the use of cloud computing technology. First is the corporate compliance (including any attorney-ethics compliance), which doesn't go away simply by switching to the cloud. Secondly, the ramifications of the loss of data (or the loss of the data *and* the provider) can be profound. Finally, there are the electronic discovery issues to be considered.[9]

Compliance issues

"CIOs must understand that data backup and storage in the cloud do not remove a company's responsibility for the legal, regulatory and audit obligations attached to that information."[10] Industry experts warn enterprises to settle several important compliance issues within the terms of the service agreement.[11]

States such as Texas have additional requirements that are not obviated by the choice of storage mechanism. Cloud-stored data is still subject to Breach/Notification laws, such as Section 521 of the Texas Business & Commerce Code.[12] Moreover, storage of sensitive information, such as

Social Security Numbers, is also subject to the same protection requirements of all Texas businesses – regardless of whether it is on the cloud or not.[13]

Loss of data

Putting your data on the cloud places reliance on the data's integrity and existence in the hands of another party, namely the service provider. Depending upon your IT infrastructure, such reliance can be a sensible or negligent. Many service providers have good records of data retention. However, mistakes are made. For example, in October 2009, Microsoft's cloud storage facility -- aptly named "Danger" -- suffered a catastrophic failure, affecting more than one million T-Moble Sidekick users for weeks.[14] Microsoft took herculean efforts to retrieve the data, with marginal success. However, the damage was done.

Loss of data need not be permanent in order to affect business operations. Even a temporary loss of access is enough to cripple critical business processes. Large organizations can require certain levels of performance from a service provider, normally in the terms of a *service level agreement* ("SLA"). The SLA can stipulate the amount of "down time" that the provider is allowed, as well as other conditions. Unfortunately, only those organizations with sufficient bargaining power can negotiate adequate SLA's. For the rest of us (and that includes most law firms), the contracts from the service providers are on a "take it or leave it" basis, with terms naturally in the provider's favor. For all organizations, big or small, it behoove the user to identify

Loss of service provider

Worse than the loss of some data is the loss of the service provider entirely. While striving to appear like the Rock of Gibraltar, many service providers content with buggy software, unreliable equipment, razor-thin profit margins, and faulty business models.

Loss of dominion

Who owns the data? Note, while the Copyright Act often does not help a third-party provider from obtaining ownership of the data, they often turn to contract clauses to obtain the same effect. Some agreements stipulate that the service provider owns the data that is uploaded and stored on their servers.

With loss of dominion comes a certain loss (or change) of responsibility. Who is responsible for the loss of data? Who indemnifies whom for a loss? Both of these questions are often addressed in the contract between the service provider and the author of the data (the client). However, in many contracts, the risks are not adequately addressed or allocated within the contract. For these reasons, some industry experts caution clients from relying too heavily upon cloud providers.[15]

Worse, with the loss of dominion come increased problems with the preservation of documents relevant to litigation, and the corresponding problems with responding to discovery requests during litigation.

Electronic Discovery

Electronic documents and other electronic information are central to every legal matter – even for those matters that do not involve litigation.[16] Lawsuits are an inevitable cost of doing business. Consequently, production of electronically stored information ("ESI") is also inevitable. Prudent shoppers of cloud resources should conduct a "dry run" of the production capabilities in order to test the provider's

capabilities and shortcomings, as well as what resources are needed within your organization (or third party expertise).

For matters involving litigation (potential or real), an extra duty – preservation – is imposed upon the party.[17] Spoliation of evidence, when there is a duty to preserve it, can prompt a court to impose sanctions on you (the attorney) and/or your client under FRCP Rule 37 (or the state equivalent).[18] Sanctions are often monetary,[19] but other sanctions include: the striking of pleadings,[20] default judgment,[21] dismissal of the case[22] or the imposition of an adverse inference instruction to the jury.[23] Preservation efforts can be especially difficult when the data is on the cloud, and preservation of metadata (or the data itself) is difficult.[24] Fortunately, Rule 37 has some safe harbor provisions, and the general rule is that sanctions will apply to intentional/willful misconduct, not mere negligence.[25] However, willful blindness allowing for destruction of evidence is not a viable solution.

Computer forensics

Cloud computing complicates computer forensics (the traditional "first step" in electronic discovery). While there are excellent forensic tools for imaging[26] and searching data, storing the data on the cloud renders many of those tools obsolete. In addition, *multiple* organizations are involved in the typical Internet presence, such as web server provider, Internet service provider, email provider, telecommunications companies, router providers and others. Consequently, forensic examiners and attorneys must attempt to gather information from disparate organizations (often outside their normal jurisdiction) via subpoena or warrant. Unfortunately, by placing another organization in the e-discovery loop – with the data stored outside the direct control of the responding party – the discovery process is inhibited.[27]

An example of complicated e-discovery involving cloud computing is a litigant whose server may in fact be a "virtual" server that is running on a large machine shared by multiple organizations, making the acquisition of a forensic image difficult, if not problematic.[28] Moreover, the fact that the data is stored on the cloud can complicate admissibility of the evidence.[29] The attorney *must* understand any extra cloud-based problems before conducting the Rule 26(f)[30] conference with opposing counsel.

For the computer forensics examiner, the shift will be from traditional examination of "dead" personal computers to gathering data from "live" servers for later analysis and presentation. More in-person testimony is likely because the evidence will need to be authenticated using (ironically) the older rules of evidence, specifically Rule 901(b)(1). Examiners can expect to see criminals (and their tech-savvy civil counterparts) use volatile RAM applications to avoid leaving traces of their activities. The key problem for the examiner, however, is the same one that so bothers lawyers – the lack of control over the data/machines that are to be examined. This puts a greater emphasis on logging information about user-activities for subsequent investigation. In general, however, the forensic examiner/ expert witness will have to:

- Identify the parties involved with the litigant's Internet presence;
- Systematically collect and time-stamp the evidence which identifies those parties;
- Save and package the evidence;

- Create a cryptographic hash value of the evidence packet to ensure its integrity; and

- Create a verifiable report that presents the identities of the parties (and any contact information) for presentation at trial or to counsel.

Fortunately, there are many Unix-based tools that lawyers and forensic experts can use to identify parties with potentially relevant evidence.[31]

Case law

An early case regarding cloud-held information subject to discovery is *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008). The opinion was related to a wrongful death suit, where the City was accused of covering up a murder of the plaintiff's relative. Earlier, the Court had allowed production of text messages held by a SkyTel, a third party provider. In this particular decision, the Court ruled upon motions to prevent the discovery of the text messages from going forward. The moving defendants argued that the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq., wholly precludes the production in civil litigation of electronic communications stored by a non-party service provider (SkyTel). The court rejected this proposed reading of the SCA, observing that "[d]efendants' position, if accepted, would dramatically alter discovery practice, in a manner clearly not contemplated by the existing rules or law, by permitting a party to defeat the production of electronically stored information created by that party and still within its control – information that plainly is subject to civil discovery, see Fed. R. Civ. P. 34(a)(1) – through the simple expedient of storing it with a third party." Because the Court felt that the SCA did not require the preclusion of discovery in such a situation, he allowed the discovery to proceed.

Another case that highlights the potential pitfalls of cloud computing is *Easton Sports, Inc. v. Warrior LaCrosse, Inc.*, 2006 WL 2811261 (E.D. Mich. Sept. 28, 2006). In this corporate espionage case, an employee of the defendant purposefully inactivated his cloud-based Yahoo! email account which "resulted in the destruction of Yahoo records concerning his computer use." As a result of this act and some other misconduct, the Magistrate in that case recommended an adverse inference instruction as a sanction.

If there is one case that highlights the distinction between "traditional" email and cloud-based email, that case would be *United States v. Weaver*, 2009 WL 2163478 (C.D. Ill. July 15, 2009) (Not Reported). In *Weaver*, the Court ruled that previously opened emails that were stored for less than 181 days in *web-based* email account could be obtained using only a trial subpoena, rather than a warrant. The Federal government sought to obtain emails and other information from a defendant's Hotmail account via a trial subpoena seeking production of "'the contents of electronic communications (not in 'electronic storage' as defined by 18 U.S.C. § 2510(7)' and specified that the '[c]ontents of communications not in 'electronic storage' include the contents of previously opened or sent mail.'" Microsoft, however, felt that a warrant, rather than a trial subpoena, was necessary to compel production, citing their local Ninth Circuit precedent *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003). In distinguishing *Theofel*, the *Weaver* court pointed out the differences within subsections of the Stored Communications Act that were affected by the choice of web-based and traditional email systems – and thus disserving of disparate treatment. This case highlights the lower standards

necessary to obtain someone's web-based email records.

In those cases where a warrant is obtained, does the owner of the account need to be notified when the warrant is served on the ISP? That question was addressed in *In re United States*, — F.Supp.2d —-, 2009 WL 3416240 (D.Or. 2009). In that case, the Court concluded that "[i]n this third party context, the Fourth Amendment notice requirement is satisfied when a valid warrant is obtained and served on the holder of the property to be seized, the ISP. In this case, the ISPs were served with the warrants to obtain the relevant e-mails. The requirements of the Fourth Amendment were satisfied." As Orin Kerr observed, "Judge Mosman concluded that Rule 41 and 18 U.S.C. 2703(a) required the notice to be served on the ISP, not the account holder, as a statutory matter," although he did not question that the Fourth Amendment applied to email.[32]

Social networking sites in litigation

Personal blogs and social networking sites such as Facebook,[33] Twitter[34] and MySpace,[35] are treasure troves of information about individuals. Users place pictures of themselves, and often very personal information on these sites. Companies have begun to use the sites as screening tools for job candidates.[36] Law enforcement agencies have used the sites repeatedly during investigations.[37] Lawyers access these sites to gather evidence for lawsuits,[38] or to screen potential jurors during *voir dire*.[39]

There are several ethical considerations with respect to social networks. Recently, the Philadelphia Bar Association's Professional Guidance Committee released an opinion on the matter, specifically about posing as someone (a "friend") in order to secure evidence for litigation.[40] A recent conference highlighted the legal and ethical problems with certain aspects of cloud computing, namely the Boalt School of Law at the University of California, Berkley held a seminar entitled "Social Networks: Friend or Foes? Confronting Online Legal and Ethical Issues in the Age of Social Networking". The law school graciously posted audio excerpts of the presentations as well as links to other materials.[41] These materials form a corpus of core materials on this subject, and would be an excellent starting point for research on the topic.

Conclusion

This paper has highlighted some of the benefits and problems associated with cloud computing. The various footnotes provide starting points for additional research into specific topics. However, there are other topics that are germane to cloud computing, but were not addressed herein, such as compliance with Federal Trade Commission ("FTC") rules, compliance with the Health Insurance Portability and Accountability Act ("HIPPA") and other privacy, trade or securities laws. Each cloud user must decide which laws are applicable to them, and appreciate the duties imposed and benefits afforded.

---

[1] Attorney at Law. B.S. Aerospace Engineering, University of Michigan, 1982; M.S. Aerospace Engineering, University of Michigan, 1984; J.D. University of Houston Law Center, 1991. Ron is admitted to practice in Texas, the U.S. District Courts for the Southern District of Texas and the District of Nebraska, the Court of Appeals for the Federal Circuit, and the U.S. Patent and Trademark Office. Ronald Chichester, P.C. is a Houston-area law firm providing counsel to law firms and companies on a wide variety of technology-related matters, including electronic discovery, intellectual property, computer forensics, electronic commerce, and corporate computer policies and procedures. Visit the firm

website at www.txcomputerlaw.com. A copy of this paper is available at his website: http://www.txcomputerlaw.com/presentations/

[2] Read more about Google Wave at: http://wave.google.com/help/wave/closed.html

[3] The specific definition for cloud computing varies. For instance, Wikipedia uses several sources in its definition of cloud computing. Specifically, they say "Cloud computing is Internet- ("cloud-") based development and use of computer technology ("computing"). In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them. It typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet." "Cloud Computing," Wikipedia, which is available at: http://en.wikipedia.org/wiki/Cloud_computing (with interla

[4] *See*, Nicolas Carr, "THE BIG SWITCH: REWIRING THE WORLD, FROM EDISON TO GOOGLE" (W.W. Norton & Co., 2009).

[5] Such network capable devices include traditional laptops ands workstations, as well as newer and smaller devices such as netbooks, iPhones, iTouch, Blackberrys, cellular telephones, etc.

[6] "Bandwidth" is the term of art for the network (Internet) connectivity between the provider's server and the user's machine. Oftentimes, the provider charges for both the storage space (to store the data) and the bandwidth needed to access that data. Other providers allow limited amounts of disk space for free, but sell advertising space on the web pages rendered to the user with their data. Still other providers give away limited amounts of disk space and/or bandwidth for free, but charge for additional space/bandwidth.

[7] "Cloud Computing Risk Assessment" European Network and Information Security Agency (November 20, 2009), a copy of which is available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/

[8] *Id*. at 4.

[9] David Navetta, "Legal Implications of Cloud Computing - Part One (the Basics and Framing the Issues)" published on llrx.com on September 12, 2009, available at: http://www.llrx.com/features/cloudcomputing.htm

[10] Linda Tucci "Addressing Compliance Requirements in Cloud Computing Contracts" on SearchCIO.com on June 11, 2009, available at: http://searchcio.techtarget.com/news/article/0,289142,sid182_gci1359026,00.html

[11] Some sample questions to ask of the cloud provider are:

Standard General Contract Issues

A. For those organizations with no bargaining power, do you have a "default" contract or standard template? If so, can I see it?

B. What are your backup procedures?

C. With respect to "uptime," what are your rates for the different "9's"?

D. In what format is the data stored on your servers?

E. In what format is it possible to export the data from your hosted service?

F. Do you charge for reformatting the data back for export into commonly used software applications (like Word and Excel)?

Security

G. What security measures are implemented by default?

H. What additional security measures are available?

I. Can we use a VPN? SSH? SFTP?

J. What type of encryption do you support?

K. Who will have access to the data?

L. How can you govern who has access to the data?

M. How can we govern who has access to the data?

N. How granular are the various levels of access to the data? (e.g, full rights for some, limited for others, none for the rest?)

O. Who within your organization will have access to the data?

P. How do you ensure that those within your organization will not compromise the security and integrity of the data?

Q. To implement any (and all) security protocols, what software applications do we need for our users?

Data Ownership

R. Do you claim any ownership rights to the data that we store on your servers? If so, what rights would you claim?

Data Retention/Electronic Discovery

S. Can you implement non-standard "tailored" document retention policies?

T. Can the tailored document retention policies implement selective litigation holds?

U. Can litigation hold-related transactions be logged?

V. What happens if I need to preserve data? Do we need to enlist you to make certain data "read only"?

W. What metadata do you keep about the data?

X. How do you preserve/produce system metadata for the documents stored on the system?

Y. What kind of user/document logging do you track? (e.g., who accessed what, and what did they do with it.)

Z. Are there any additional logging options?

AA. How is the data collection to be done if I need to produce data during litigation?

BB. Who can/will produce the data? (I.e., will we be able to produce the data ourselves? Our third-party expert? Or must we rely on you?)

CC. How much do you charge for identifying/searching/processing/producing the data?

DD. Given that "preservation" of documents and their metadata kick in almost immediately after litigation commences, how soon can you implement a litigation hold notice?

EE. After getting a subpoena, how long does it take for you to produce data?

Privacy

FF. Which jurisdictions are your data centers in, and how is privacy protected in those jurisdictions?

GG. How do you respond to governmental requests for information about your data?

HH. Would you warn us if the government issues a subpoena?

II. How can you ensure that cross-border legal (privacy) limitations on storage of data are met?

[12] See, specifically, Sections 521.002 (Definitions), 521.052 (Business Duty to Protect Information), and 521.053 (Notification Required Following Breach of Security of Compromised Data); a copy of the text of the statute is available at: http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm

[13] See specifically, Texas Business & Commerce Code §501.001 (Certain Uses of Social Security Numbers Prohibited), §501.001 (Remedies), §501.052 (Privacy Policy Necessary to Require Disclosure of Social Security Numbers) the latter of which stipulates that the person providing the social security number be afforded a policy by the requestor indicating where the data will be stored, and how it will be protected, and §501.053 (Remedies). A copy of the statute is available at: http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.501.htm

[14] Eric Zelman, "Cloud Goes Boom, T-Mo Sidekick Users Lose All Data", InformationWeek, October 10, 2009 available at: http://www.informationweek.com/blog/main/archives/2009/10/cloud_goes_boom.html. *See also*, Rich Miller, "The Sidekick Failure and Cloud Culpability," Data Center Knowledge, October 12, 2009, available at: http://www.datacenterknowledge.com/archives/2009/10/12/the-sidekick-failure-and-cloud-culpability/. *But see*, Sam Johnson, "If it's dangerous it's NOT cloud computing" available at: http://samj.net/2009/10/if-its-dangerous-its-not-cloud.html (it's not the cloud that's bad, it was the components without sufficient redundancy that was the real culprit).

[15] Henry Newman, "Why Cloud Storage Use Could Be Limited in Enterprises" Enterprise Storage Forum, October 9, 2009, available at: http://www.enterprisestorageforum.com/technology/features/article.php/3843151

[16] Ronald Chichester, "The Collection Process: Collecting Evidence or Collecting Sanctions" at 1, AccessData White Paper (2009), available at: http://www.accessdata.com/downloads/media/Collecting_Evidence_or_Collecting_Sanctions.pdf

[17] *Id*. "The duty to preserve evidence 'arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.'" *Acorn v. City of Nassau*, 2009 WL 605859 at 2 (E.D.N.Y. March 9, 2009) citing *Zubulake v. USB Warburg LLC* ("*Zubulake IV*"), 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (which itself quoted *Fujitsu Ltd. v. Federal Express Corp*., 247 F.3d 423, 426 (2d Cir. 2001). "Once the duty to preserve arises, a litigant is expected, at the very least, to 'suspend its routine document and retention/ destruction policy and to put in place a litigation hold.'" *Id*., citing *Zubulake IV*, 220 F.R.D. At 218; and see also *Doe v. Norwalk Cmty. Coll*., 2007 U.S. Dist LEXIS 51084, at *14 (D. Conn. July 16, 2007) (A party needs to take affirmative acts to prevent its systems from routinely destroying information).

[18] Federal Rules of Civil Procedure ("FRCP") Rule 37 (Failure to Make Disclosures or to Cooperate in Discovery; Sanctions), a copy of which is available at: http://www.law.cornell.edu/rules/frcp/Rule37.htm

[19] Chichester, supra, note 16 at 1, citing *Kipperman v. Onex Corp*., 2009 WL 1473708 (N.D. Ga. May 27, 2009) ($1,022,700.00 in monetary sanctions levied against the defendant for a "textbook case of discovery abuse.")

[20] FRCP Rule 37(b)(2)(iii): "striking pleadings in whole or in part." *See, e.g., Channel Components, Inc. v. Am. II Electronics, Inc*., 915 So. 2D 1278 (Fla. Dist. Ct. App. 2005) (striking of the pleadings considered, but not imposed by the Court).

[21] FRCP Rule 37(b)(2)(vi): "rendering a default judgment against the disobedient party." *See, e.g., Gutman v. Klein*, 2008 WL 4682208 (E.D.N.Y. Oct. 15, 2008) (Magistrate Judge recommended default judgment in favor of the plaintiff, plus attorney fees); *Atlantic Recording Corp. v. Howell*, 2008 WL 4080008 (D. Ariz. August 29, 2008) (default judgment warranted after "brazen destruction of evidence").

[22] FRCP Rule 37(b)(2)(v): "dismissing the action or proceeding in whole or in part." *See, e.g., Kvitka v. Puffin Co., LLC*, 2009 WL 385582 (M.D. Pa. February 13, 2009) (all of plaintiff's claims were dismissed, and an adverse instruction was awarded to the defendant's cross-claims after the plaintiff intentionally discarded her laptop in spite of a duty to preserve it.).

[23] *See, e.g., Smith v. Slifer Smith & Framption/Vail Assocs. Real Estate, LLC*, 20009 WL 482603 (D. Colo. February 25, 2009) (despite lack of evidence of a "smoking gun," the Court awarded an adverse inference against the defendant because some documents were destroyed well after the litigation hold notice was put in place.)

[24] *See, e.g., Easton Sports, Inc. v. Warrior LaCrosse, Inc.*, 2006 WL 2811261 (E.D. Mich. Sept. 28, 2006) (adverse inference sanction awarded when defendant intentionally deactivated their cloud-based Yahoo! email account).

[25] *See, e.g., Gippetti v. UPS, Inc.,* 2008 WL 3264483 (N.D. Cal. Aug. 6, 2008) (Court declined to impose sanctions because the conduct in question came under one of the safe harbor provisions).

[26] Imaging, in computer forensic parlance, is the practice of making an exact duplicate (bit-for-bit) of a hard disk or a portion thereof, thereby preserving the electronic evidence. Imaging is an excellent way to prevent spoliation of the evidence, and to avoid subsequent sanctions by the court.

[27] John J. Barbara, "Cloud Computing: Another Digital Forensic Challenge" DFI News, October 27, 2009, available at:
http://www.dfinews.com/articles.php?pid=716
See also, Christine Taylor, "The Cloud and eDiscovery", NetworkComputing.com, July 30, 2009, available at: http://www.networkcomputing.com/e-discovery/the-cloud-and-ediscovery.php
For an cloud-industry spin on the topic, *see* Dan Morrill, "Cloud Computing Making Forensics Easier" Cloud Ave., September 22, 2008, available at:
http://www.cloudave.com/link/Cloud-computing-making-forensics-easier (Cloud computing makes forensics *easier* because you can backup key evidence files onto the cloud for preservation).

[28] Barbara, *supra*, note 27. For more information about virtual machines (which act as virtual servers), see:
http://en.wikipedia.org/wiki/Virtual_machine

[29] Phillip Malone, "Social Networking Evidence: Sources, Authentication and Admissibility" H2O Playlist Bets, November 23, 2009, available at:
http://h2obeta.law.harvard.edu/315300

[30] FRCP Rule 26(f), the so-called "Meet & Confer" conference in which, under the amended Federal Rules, opposing counsel identify where data is stored, and any potential problems with the searching and production of that data. Several states have their own equivalents.

[31] For an excellent article that describes the basic network forensic process, see Nikkel, Bruce J. "Domain Name Forensics: A Systematic Approach to Investigating an Internet Presence," Digital Investigation: The International Journal of Digital Forensics and Incident Response, Vol. 1, No. 4 (oid:10.1016/j.diin.2004.10.001) (August 1, 2005). A copy of the article is available at:
http://www.digitalforensics.ch/nikkel04.pdf

[32] Orin Kerr, "District Judge Concludes E-mail Not Protected by Fourth Amendment (But See Correction)" The Volokh Conspiracy, October 28, 2009, available at:
http://volokh.com/2009/10/28/district-judge-concludes-e-mail-not-protected-by-fourth-amendment/

[33] http://www.facebook.com For an example of things to be concerned about if you or your employees use FaceBook, *see*, Jamie N. Nafziger and Kelcey Patrick-Ferree, "Don't just close your eyes and leap: top five issues in the Facebook terms of use" ACC Lexology, October 9, 2009, available at: http://www.lexology.com/, and James D. Heeney and Sharaf Sultan "Social networking: what employers need to know" ACC Lexology, October 14, 2009, also available at: http://www.lexology.com/

[34] http://twitter.com

[35] http://www.mayspace.com

[36] *See, e.g.*, "The pitfalls of Social Networking Websites," McLaughlin Investigative Group, available at:
http://www.mclaughlinpi.com/blog/?p=25

[37] *See, e.g.,* Mandy Locke, "Police increasingly use Myspace-like sites as investigation tool" PoliceOne.com, July 16, 2007, available at: http://www.policeone.com/investigations/articles/1290064-Police-increasingly-use-Myspace-like-sites-as-investigation-tool/

[38] *See, e.g.,* "Social Networking Sites and Litigation," Adjunct Law Prof Blog, September 11, 2009, available at: http://lawprofessors.typepad.com/adjunctprofs/2009/09/social-networking-sites-and-litigation.html

[39] *See, e.g.,* "Why you need to know whether your jurors blog" on the blog *Deliberations*, November 12, 2008 available at: http://jurylaw.typepad.com/deliberations/voir_dire_questions/

[40] The Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02 (March 2009), available at: http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf. That opinion also cited: citing "Deception in Undercover Investigations: Conduct Based v. Status Based Ethical Analysis," 32 Seattle Univ. L. Rev.123 (2008), and "Ethical Responsibilities of Lawyers for Deception by Undercover Investigators and Discrimination Testers: An Analysis of the Provisions Prohibiting Misrepresentation under Model Rules of Professional Conduct," 8 Georgetown Journal of Legal Ethics 791 (Summer 1995).

[41] The links and other materials are available at: http://www.law.berkeley.edu/institutes/bclt/socialnetworking/schedule.htm See specifically the audio recordings of "Problems Unique to Social Networking and the Law", "Does Overt Access to Social Networking Data Constitute Spying or Searching?", "Are You Really My Friend? The Law and Ethics of Covert or Deceptive Data-Gathering", "MyFace in Court: Admissibility and the Probative Value of Social Networking Evidence", "Regulating Crime in the Cloud: Policing Unlawful Behavior on Social Networks", and "Can Lawyers "Tweet" About Their Work? Confidentiality & Legal Professionalism in the Age of Social Media".