

# Disaster Recovery Planning

Presented by

**Alan Friedman, CPA**  
Friedman, Kannenberg & Company, P.C.



# Objectives:

- ✦ Identify the “**kinds of disasters**” to prepare for
- ✦ “**Tales of Survival**” from some people we know
- ✦ How to prepare a “**Disaster Recovery Plan**”
- ✦ Did we “**learn**” anything?

# **“Disasters” come in three different types:**

 **Acts of “God”**

 **Acts of  
“Human Error”**

 **Acts of “Terror”**

Disasters  
from

**“Acts of God”**

# Earthquake



# Hurricane



# Flood



# Tornado



# Fire



# Tsunami



# Lightning



# Power Outages/Blackouts

# Mudslide



# Snow



**Disasters  
from**

**Acts of  
“Human Error”**

# Computer Failures



# Internet and Systems Failure



# Lawsuits

Billboard

## Opinion

*The Record Industry Has Fallen Behind The Curve On Internet File Sharing*

# Lawsuits Are A Necessary Evil

Laws must be enforced against violators, or eventually the general public begins to forget that the laws exist, and chaos ensues. This is as true for copyright law as it is for laws against jaywalking and shoplifting.

If no one ever stopped people from walking out with free food from the corner store, eventually no one would patronize the other supermarkets and everyone would just go to the corner store.

The record industry, whether due to arrogance or ignorance (or a little of both), fell behind the curve on the Internet file-sharing issue.

While the record companies looked the other way, there was a cultural shift in the public's mindset. Everyone began to view the Internet and its seemingly unlimited access to everything as a new

frontier without limits.

Consumers came to believe that if you could get it on the Internet, it was acceptable to get it for free.

As the record companies have learned, it is difficult to compete with "free"—but they should not

copyright infringement.

Taking music for free from the P2P file-swapping networks is the Internet equivalent of shoplifting from a record store that stole the records from a warehouse in the first place.

The economics of the record business were getting desperate. The copyright law had to be enforced in a series of high-visibility lawsuits to not only stop those particular infringers but also to send a strong message of deterrence to all of the other violators.

The message finally seems to be getting across the cultural divide.

To some extent, many of the violators may be adolescent, "innocent" infringers unaware of the copyright law.

That excuse will no longer apply, particularly because many of the infringing downloaders are so young that, in fact, it is their parents who would be held

liable in court.

Those parents read the news and, it is hoped, have gotten the message. A recent news report indicated that thousands of downloaded files have been deleted. Parents across the country are presumably now instructing their children at home not to download illegally on the family computer.

This is precisely the deterrent effect that the record company lawsuits were meant to have. Litigation can be an extremely effective educational tool in that way.

Let's hope this message will spread to law-abiding parents, who will properly instruct their children not to violate the copyright law just as they instruct their children not to jaywalk or shoplift.

This may seem a bit idealistic, but then laws themselves, as a concept, are also fundamentally idealistic.

Citizens co-exist in a society

because they agree to respect one another's rights and obey the law. Contrary to the many naysayers, I believe that the record companies did what they had to do.

The lawsuits are a necessary evil that will, hopefully, have the desired effect in the long run and bring the industry back from the edge of the abyss.

Over time, the record industry will adjust its business model to accommodate legitimate downloads and will stop hemorrhaging money.

The gloomy forecasts will dissipate, and profitable outlooks will again dominate corporate balance sheets so that talented artists can be nurtured, funded and encouraged to make great music for which they will be justly rewarded.

*Wallace Collins is an entertainment lawyer with the New York firm of Serling Rooks & Ferrara.*

Taking  
Issue

By Wallace Collins



TAX ON RETURN	\$28,627.27
TOTAL CREDITS	\$ .00
AMOUNT PREVIOUSLY REFUNDED TO YOU	\$ .00
UNDERPAYMENT	\$28,627.27
*PENALTY	10,305.82
*INTEREST	1,808.01
AMOUNT YOU OWE	\$40,741.10

# Dishonest Competition

## **Illinois piano dealers square off in court; Biasco pianos and five other dealers trade charges of deceptive trade practices**

[Music Trades](#), [September, 2003](#)

 PREMIUM

REFLECTIVE--IF NOT symptomatic--of the piano market's harsh business climate, six Chicago-area dealers recently filed suit against one of the area's dominant competitors for what they claim to be violations of the Illinois Deceptive Trade Practices Act. The plaintiffs--Cordogan's Pianoland, Hendricks Piano, Karnes Music Co., Ortigara's Musicville, and Pickle Piano Co.--are seeking injunctive action against Event Marketing Group, Inc. d/b/a Biasco Piano Company. Biasco, in turn, has filed a verified counterclaim against Cordogan's Pianoland and Pickle Piano Co. Below is a synopsis of the plaintiffs' complaints. (Counterclaim complaints follow.) Many of the plaintiffs' charges pertain to Biasco's advertisements, which they contend: ...

# Bad Press

## St. Petersburg Times

### FLETCHER MUSIC UNDER FRAUD INVESTIGATION

**MusicTrades** Music Trades; 9/1/1998

FLETCHER MUSIC CENTERS, the 31-store Florida based home organ chain, is currently under a wide-ranging fraud investigation that was triggered by the actions of Jeffrey Snyder, a top performing salesman and store manager. As reported by the St. Petersburg Times, Snyder allegedly persuaded customers to give him money that he promised to invest for them in Fletcher stock, once the company went public. The Times noted that as of early July at least 64 Fletcher customers were involved in the phony stock sale and that their losses totaled more than \$1.3 million. Snyder awaits trial on 11 ...

# Loss of Credit

## Mars Music Files for Bankruptcy

September 28, 2002

---

Advertisement

---

According to a recent report by the Miami Herald, the Mars Music ([www.marsmusic.com](http://www.marsmusic.com)) superstore chain filed for Chapter 11 bankruptcy protection on Friday.

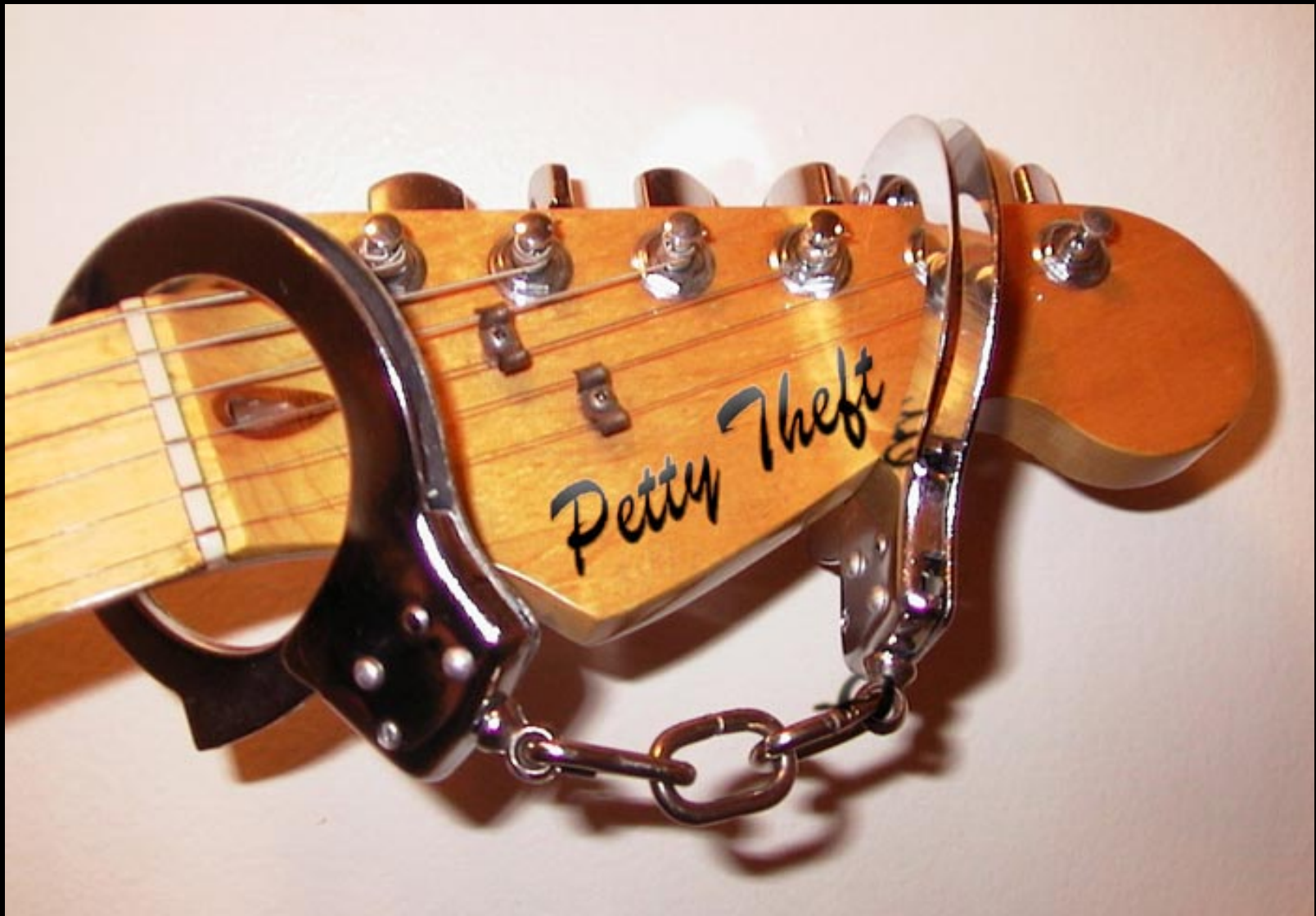
**Disasters  
from**

**“Acts of  
Terror”**

# Arson



# Robbery



# Internal Fraud



# Identity Theft



# Terrorism



A dark, stormy sky with a bright lightning bolt striking down. The lightning bolt is a bright white line that starts from a cluster of white clouds in the upper right and extends vertically towards the bottom center of the frame. The surrounding sky is dark and filled with swirling, greyish clouds, creating a dramatic and intense atmosphere.

# How do you protect yourself and your company ??

**By creating a solid and  
*constantly evolving*  
“Disaster Recovery Plan”  
(DRP)**

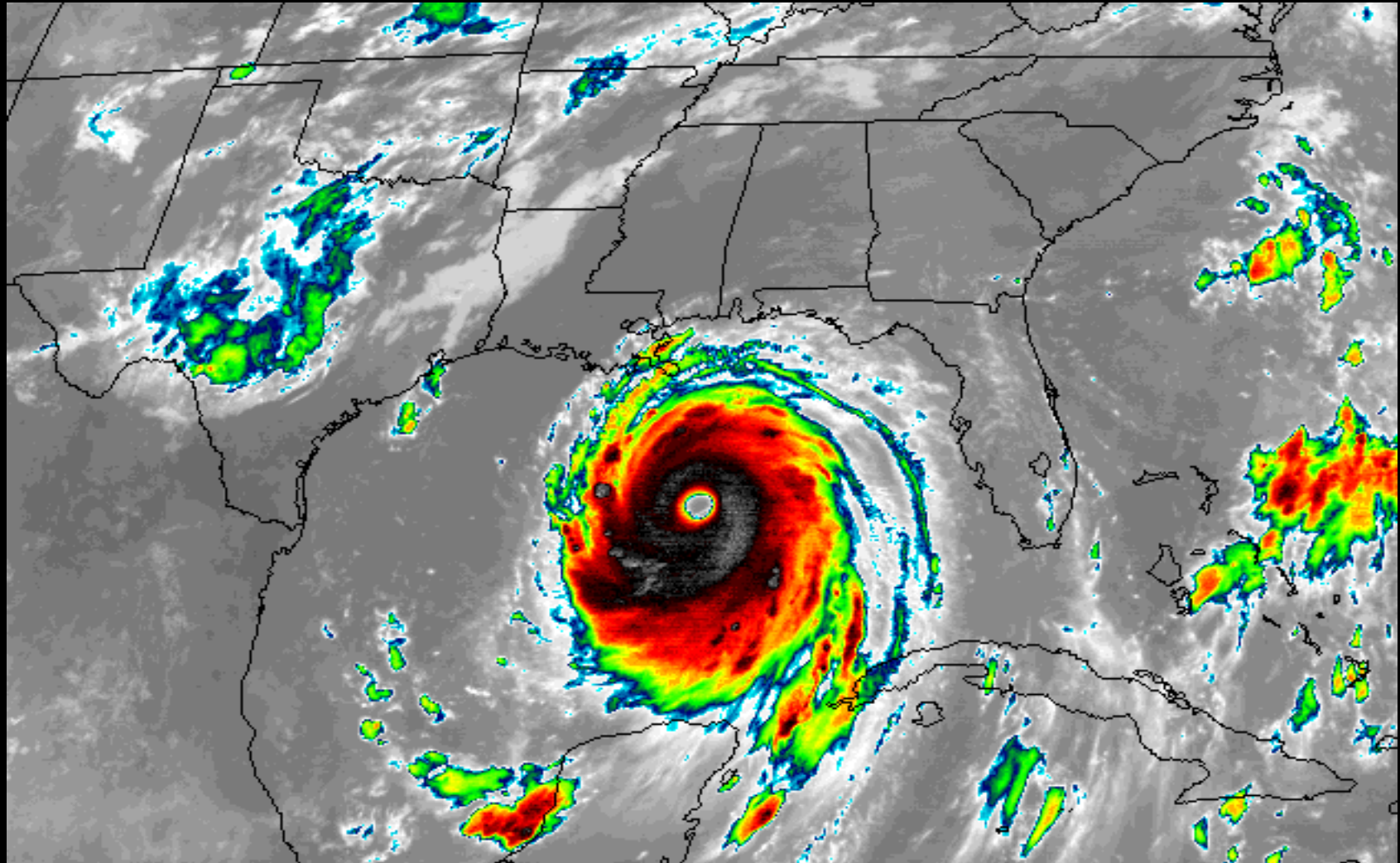
“Why do I have to do this?”

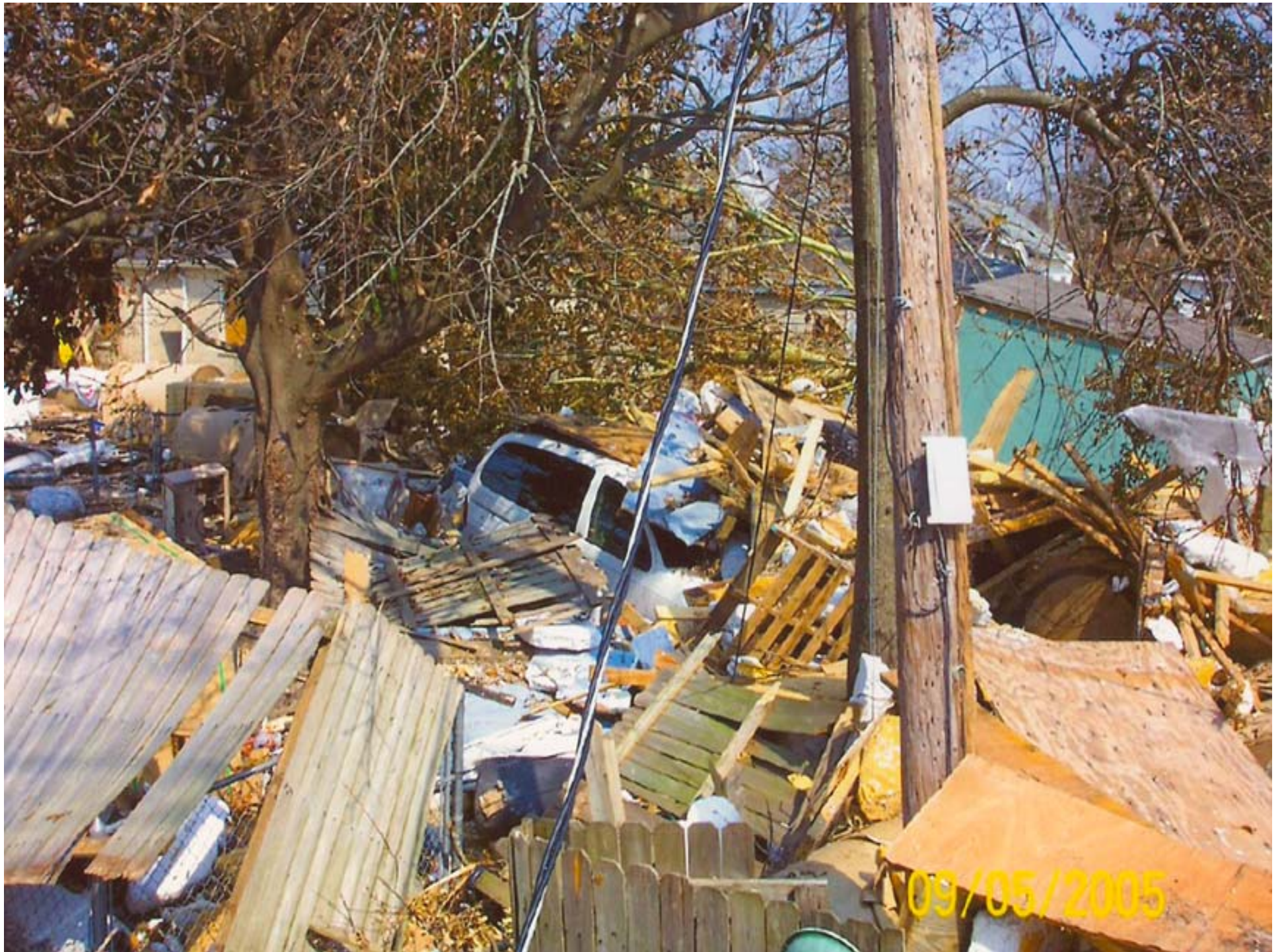
“What really are the chances of something happening?”

“It’s a waste of time & money preparing for the unknown.”

“I’m pretty sure we’d know what to do if disaster strikes.”

# **"The Aftermath from Hurricane Katrina"**













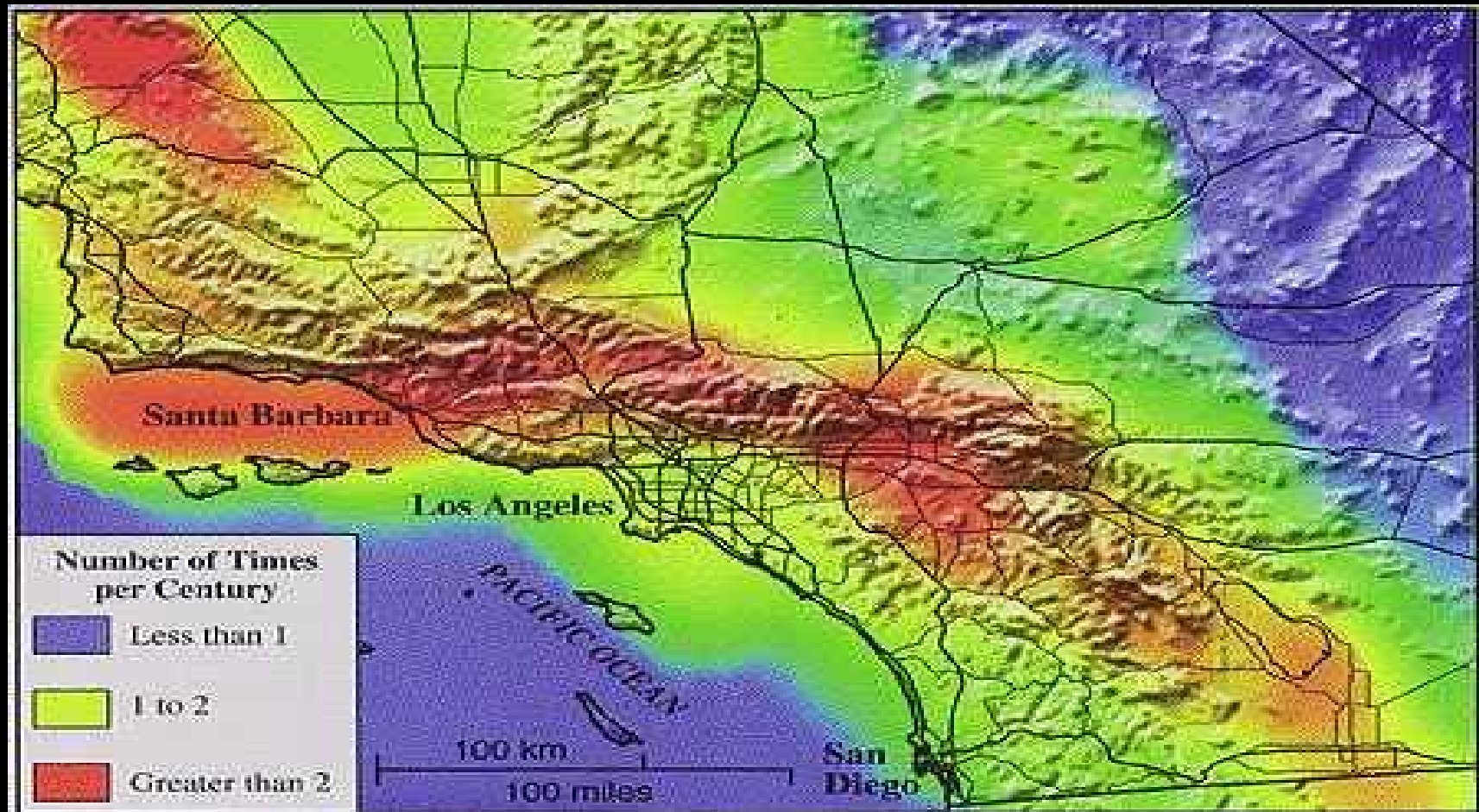








# Alfred Publishing's Survival from the Northridge Earthquake



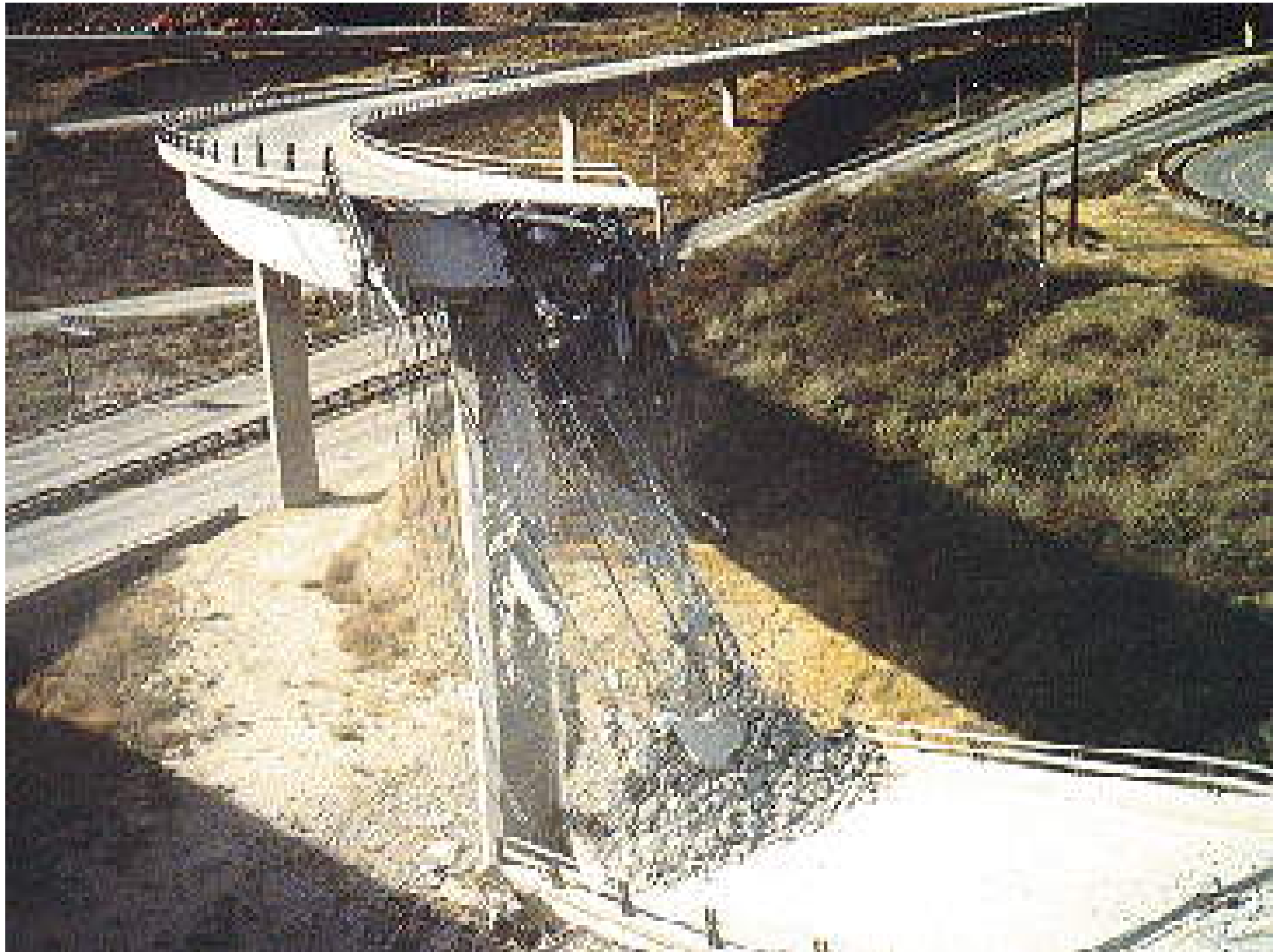


















Photo: 10/26/2014 11:11 AM



















# Keep in mind...

- Disaster Recovery Planning (“DRP”) has always been important to large companies, but is no less important to smaller ones
- As we’ve all become more (or perhaps even “totally”) reliant on technology, DRP is now “essential” for every company, regardless of size
- For disaster recovery to be truly successful, it must be viewed as a “dynamic process” (one that changes as our world changes), and our DRP must constantly be monitored, tested and reevaluated

So, to create a DRP  
that really works,  
the individuals  
creating the DRP must  
truly be able to think  
“outside the box”...

**The “Goal” of disaster  
recovery is simple:**

**“To guarantee that your  
business, large or small,  
can survive “any”  
internal or external  
emergency.”**

**We can accomplish this  
by addressing three  
“key” questions...**

- (1) How can the company recover it's most critical data and resources?**
- (2) How can the company resume it's “mission critical” workflow?**
- (3) How can the company execute the contingency plans necessary to accomplish items #1 and #2 above?**

**Implementing a  
“Disaster Recovery  
Plan” should be  
approached in the  
following “7 steps”  
using imagination,  
brainstorming and  
forethought ...**

# **"7 Steps" to Implementing a DRP...**

- (1) Identify Your Critical Assets**
- (2) Evaluate a Disaster's Impact**
- (3) Develop Strategies to Survive**
- (4) Design DRP around 1, 2 & 3**
- (5) Implement the Plan**
- (6) Train Your Employees**
- (7) Test the Plan**

# **1. Identify Components and Resources Critical to your Business**

- The most critical component in today's business environment is usually financial and operational "data" (i.e. customer lists, inventory records, accounting transactions)
- Most of this data is recorded on electronic media (i.e. computer hard drives) which, while reliable, is not free from errors when exposed to heat, water and other elements

# **1. Identify Components and Resources Critical to your Business**

- Because disasters generally occur in regions, it's important your data is backed up often and moved far enough offsite from your area of original processing (think about the wide destruction of hurricanes).
- You can't just rely on your computer system to tell you your backup was successful; you need to test it to make sure you have the correct hardware and software versions on backup computers.

## **2. Evaluate What Impact a Disaster Will Have on Your Business**

- Ask yourself: "What if the worst happened? How would it affect my business, my family, my employees and their families? Would we survive if the business were closed for days, weeks, months, or perhaps my entire "school music" or "holiday" season?"
- Be pessimistic and assume a myriad of disasters CAN and WILL happen to you; develop a DRP that allows you to keep the doors open under all kinds of possible disaster scenarios

### 3. Develop Business Continuity Strategies

- Develop effective business strategies by asking yourself critical survival questions:
  - What do I do if my store is completely destroyed?
  - Could I operate out of my home or from a nearby storefront?
  - Could I quickly transport critical items, such as computers and inventory, to a new location, or can I use my home, and home computer and phone line?
  - How quickly can I get product from my vendors, and on what payment terms?

### 3. Develop Business Continuity Strategies

- What if there's a prolonged power outage? What if my key suppliers are shut down, even though I'm not? What if all of my customers suffered a disaster and no longer needed any of my products and/or services?
- What if "all" phone lines are out and I can't communicate with my employees, customers, suppliers or those people I'm going to need to help me get my business back up and running?

## 4. Design a DRP to Meet the Specific Needs of Your Business

### OPERATIONAL TIPS:

- Purchase a backup generator to maintain full operations or critical functions, such as lighting, security and computer systems.
- Have backup vendors in case your primary ones are disabled. Set up relationships in advance, and maintain them by placing occasional orders so they regard you as an "active" customer when you need them; minimize loss by diversifying cust, prod, svc.

## 4. Design a DRP to Meet the Specific Needs of Your Business

### COMMUNICATION TIPS:

- Maintain an up-to-date list of all employees, their home and cellular phone numbers, their home e-mail addresses, their computer logon IDs and all applicable passwords.
- Develop an employee “telephone tree” to enable you to rapidly contact employees in the event of an emergency, and communicate to your employees what their responsibilities are in the event of disaster.

## 4. Design a DRP to Meet the Specific Needs of Your Business

### INSURANCE TIPS:

- Review your current insurance coverage with your insurance agent to make sure you have adequate coverage to get you back in business, and review/update it annually.
- Beware of contents insurance; does it cover the “replacement” cost of your equipment?
- Know what your policy “doesn’t” cover, like flood, sewer backup and earth movement.
- Consider “business interruption” insurance.

## 5. Implement the Plan

- Planning starts at the top. The design, implementation, testing and continuous review of a DRP are part of mgt's responsibility; if you feel you can't address all disaster recovery issues within your store, get outside help.
- The plan should be in writing, in both paper and digital form (i.e. PDF format) and should be distributed to all of your employees.

## 6. Train Your Employees

- Remember, disasters can result in a loss of life and a loss of valuable people who have knowledge and expertise of your store's systems and processes; accordingly, it's essential that all job tasks are documented in writing to allow others to fill in for those who are sick, injured or missing.
- Organize a system that assures each employee knows what staff, customers, vendors, bankers, insurance agents, accountants and lawyers they are responsible to contact.

## 7. Test The Plan...Often

- Because of our heavy reliance on computers to run and manage our business operations, it's now considered "mandatory" to have either complete system redundancy or access to a sufficient number of computers in another location when disaster strikes.
- Although regularly reviewing the DRP is important, it's not enough. Without warning, spring a mock disaster on your staff. Make sure they can set up a replica data center within a few hours to prove you can be back in business in short order.

# If and when disaster strikes...

- ✦ Pull out your DRP and follow it.
- ✦ Contact your employees and determine if they need any medical, financial or psychological support.
- ✦ Organize a communication system that allows everyone to be in touch with one another.
- ✦ Start the process of getting everyone productive and restoring operations.

## **In summary, When disaster strikes...**

- ⚡ Assess your ability to continue business by creating lists of products and resources that are available to generate revenue.
- ⚡ Determine what equipment is working, what isn't, and then address your most immediate needs (space, tel svc, inventory)
- ⚡ Communicate with all of your key people (ins agent, banker, creditors, etc.), and establish an alt. postal delivery system
- ⚡ Pursue insurance claim and payment

# DRP Resources

- There are scores of websites on the internet that provide free information, guidelines and checklists for DRP; simply go to "Google" ([www.google.com](http://www.google.com)) and type in: "Disaster Recovery Planning"
- But one of the best resources I found was a 50-page document entitled "OPEN FOR BUSINESS: A Disaster Planning Toolkit for the Small to Mid-Sized Business Owner"
- You can get it at the Institute for Business & Home Safety's website: [www.ibhs.org](http://www.ibhs.org)

# Alan M. Friedman, CPA

(alan@fkco.com)



friedman kannenberg

and company pc

91 South Main Street  
West Hartford, CT 06107  
(860) 521-3790  
[www.fkco.com](http://www.fkco.com)