

Planning for Disaster, Part II by Stuart Adams

Just when you thought it was safe to read something without having to see more about disasters, here comes part two of disaster planning for businesses. As Yogi Berra said, “it ain’t over till it’s over.” (If you’re too young to remember him saying that, please feel free to verify this at www.yogi-berra.com/yogiisms.html) Unfortunately, in the case of disasters, and regardless of the outcome of the “war on terrorism,” there will always be disasters of some sort which can terminate your business “with prejudice.” In this article, we’ll try to establish some ways to actually prepare and implement a disaster plan.

SO YOU THOUGHT INSURANCE WAS THE ANSWER!

If you read last month’s article, you may have felt that disasters were pretty much inevitable and something no one could reasonably plan for. You may have also come to the conclusion that insurance really was the only way to go in the event of a disaster, but a recent article by Sylvia Hsieh in *Lawyers Weekly USA* (available at www.lawyersweekly.com/usanews1105.cfm) predicts that insurance companies will become more aggressive in putting clauses in new policies which eliminate coverage of terrorist attacks. This may put you back in the position of actually having to take action, other than pulling out your wallet, in order to protect yourself, your employees and your business. Don’t discard your casualty, property damage, umbrella, business interruption or “key employee” policies just yet, but you definitely need more than them.

The *Lawyers Weekly USA* article also predicts that insurance “hot spots” will be disputes over inclusion of claims relying on the “ripple effect” of terrorism and other disasters. Businesses which were not directly destroyed or physically damaged on September 11th, 2001 have, for instance, made claims based upon total loss of business when airports were shut down and air traffic reduced, even after flights were resumed. Think, for instance of those gift shops in the concourses of airports. They rely on foot traffic which disappeared for a while and resumed at a reduced rate after the 11th. There is no doubt they were severely impacted by events which were physically remote from their shop location, but one can only ponder the possible arguments as to coverage on their business interruption insurance policy, if any. You do have some of that, don’t you?

Some types of insurance clauses you might have overlooked might be:

- “contingent interruption” (This relates to covering reimbursement for loss of a key customer or supplier, or the delay in receipt of materials needed for the business to manufacture its own products.)
- “civil authority interruption” (This might protect you if, for instance, your

- business was in the “disaster zone” and police prohibited access to it for a time, even though it was not directly damaged.)
- “war exclusion” (The application of this is debatable in the event of terrorist attacks or threats, since this usually applies only when one country is at war with another, not in the case of a terrorist group.)
 - “service interruption” (This might cover you in the event of loss of electricity, water, etc.)
 - “related expenses” (This will likely be a battlefield when categories of allowable damages will be compared to “industry standard” claims and the duty of mitigation of expenses will be explored.)
 - “duty to mitigate” (Insurance policies and courts typically require an injured or damaged party to attempt reasonable efforts to prevent further loss after discovery of the damage, but the standard of what is “reasonable” and the level of reasonable contingency planning and disaster management has probably been raised in the wake of September 11th.)

In last month’s article, I wrote about some examples of large and small “disasters” which can befall a company. Undoubtedly, in the wake of September 11th, 2001, the definition of disaster will seem different to most Americans. Our focus, in thinking about the word “disaster,” will, for the foreseeable future, probably have more emphasis on terrorist attacks than at any time in the history of our country. Certainly, we should now realize that such attacks can be a reality in this country, but we should not become so concerned with disasters of that magnitude that we forget other varieties of problems are, statistically, more likely to cause the demise of a company.

A quick review of some of the materials available at the Web site of the Institute of Crisis Management, (ICM) in Louisville, Kentucky (www.crisisexperts.com) should remind us that many companies have suffered devastating results from sexual harassment litigation and IRS audits. The archives available at this site give something of a comparison, on an annual basis, of the leading “catastrophes” suffered by businesses ICM studied. The majority seem to have been caused by employees of the company itself, either through action or inaction. Typically, vigilant management could have detected and prevented such problems, if they had educated themselves in the skills of crisis management.

CRISIS MANAGEMENT SKILLS

The management of anything requires both foresight and hindsight. Sometimes we may wonder why some companies seem to continually achieve while others wander from one crisis to another. Perhaps Thomas Jefferson had an insight when he said: “I’m a great believer in luck, and find that the harder I work, the more I have of it.” Fortunately, in the case of disaster management, there are lots of government agencies and business entities which have already put together

excellent tools for managing business risks, including terrorism, burglary, fire, flood, earthquake, tornado, hurricane, utility interruption (including loss of electricity, water, sanitation, communications such as wired and wireless phone, internet and intranet service, etc.), assault on or injury to key personnel, internal sabotage from disgruntled employee, and many more. In other words (actually quoting Yogi Berra again) you can make sure “the future ain’t what it used to be.” I don’t know what that means either, but I just had to stick it in here as a flimsy segue.

The December, 2001 issue of *Corporate Counsel* magazine (www.corpcounsel.com), published by American Lawyer Media, is chock full of good advice for lawyers pondering the fate of the many legal and financial firms which suffered damage or complete destruction in the World Trade Center attacks. Much of the advice is just as germane to any type of business, large or small, so I believe it bears repeating here. Here are some of the lessons:

- Prior to September 11th, few US businesses had disaster plans which dealt with terrorism or major disasters. With the news coverage and analysis of those events, the bar has been raised for managers of any business. Those who had disaster plans or contingency plans undoubtedly have a higher moral and legal duty to prepare for almost anything. Said another way, you may not be able to ever sleep at night again, let alone collect on your company’s insurance policies, if you have not adhered to the new “reasonable business” standard for disaster planning.
- Your employees may now appear to be functioning “as usual” on the surface, but they may be privately suffering some level of posttraumatic stress disorder. Getting, training and keeping good employees is always a challenge and major expense of any business. You may want to consider offering or facilitating extended counseling to your employees to help them cope and stay productive on the job. You might also want to consider ways to offer them greater flexibility as a “reasonable accommodation” under laws such as the Americans with Disabilities Act and The Family and Medical Leave Act. (Check out the National Mental Health Association Web site at www.nmha.org for tips on recognizing stress, such as inability to focus, irritability and anger, etc., which may, at first, seem to be unrelated to terrorist attacks.)
- The Internet was designed originally, in part, on the model of a communications system which could not be totally shut down in the event of a major disaster. This is largely due to redundancy and decentralization of resources. This is a good model or lesson, to some extent, for any business. Centralization can obviously have its drawbacks, if the central or sole location is completely destroyed or simply put out of commission for an extended period of time. Consider a “dummy office” located in your home or far enough away from the main office, which would have a “mirror” computer and communications set up. The remote site hardware and software should be compatible with that of the main office, so that backup copies of financial,

customer, project, employee, tax and other essential records can be immediately utilized. Here are a few suggestions:

THE "DUMMY" OFFICE

- mirror computer set up
- backups of data and programs
- passwords
- communications alternatives (phone, fax, e-mail, etc.)
- financial info & account numbers, checks - deposit slips
- insurance claims forms
- employee, vendor, customer contact numbers & info
- office supplies including letterhead

OTHER RISKS

While you're preparing your disaster and contingency plans, don't forget those old, pre-September 11th style disasters. Those include relying too much on a single supplier or customer, only to find you're out of business or at a tremendous disadvantage in negotiating if they depart. They also include sabotage by a disgruntled employee, theft of trade secrets, breach of non-compete agreements (I can't tell you how many times a business owner has come in to see me about this, only to find that when the key employee left to start a competing business, the original and all copies of his or her non-compete agreement was found to be missing), embezzlement, burglary, water damage (please refresh yourself on what happened in my office by reading last month's article), death or sudden disability of the owner or key employee, etc.

In order to get a good night's sleep (pun sadly intended), you might want to read *The Small Business Owner's Guide to a Good Night's Sleep*, by Debra Traverso, Bloomberg Press, 2001 Princeton, NJ. This book does an excellent job of outlining every conceivable category of business risk, at least alphabetically from advertising disasters to Web mistakes, and tells you what to do about each. It also includes a number of self audit tools and a good opening section on how to understand, assess, and control risk. Additionally, it includes a pretty good resources section at the end, which gives Web addresses by category for "Competitive Sleuthing" so your competition doesn't sneak up on you, "Employee Concerns" to help you find employees and do background checks on them, "FEMA Guidance for Free" with links or references to many key publications by that agency, "Management," noting that ICM has reported 75% of business crises can be attributed to management, "Professional Help," with links to find an attorney (presuming you would look beyond the end of your nose, a CPA, or other business professional, and several other categories.

The book does a good job of outlining even more potential business horrors than I have in this article. It contains bite sized sections on what to do if your Internet Service Provider goes out of business, there is a hazardous material spill in front of your office, your key employee dies, or you simply need to figure out how to back up, safeguard and restore your computer data. It also walks you through what it calls the most common management missteps and how to avoid them ,as well as how to foresee that “smouldering crisis” which could sack your company. The book is a quick read and a hand desk reference for any business owner or manager. I would commend it to your business library.

REALLY CHEAP RESOURCES

If you're too cheap to fork out the twenty bucks for that book, fear not. There are tons of resources available for free on the Internet to help you out. Here are a few you might peruse:

- Naturally, the Small Business Administration has articles which can be read online or are downloadable for free. On the topic of disaster preparedness, an excellent checklist can be found at www.sba.gov/disaster/getready.html. There is also a link at the root site to information on obtaining a disaster assistance loan.
- The Federal Emergency Management Agency (FEMA) has several very handy checklists and articles available at its Web site, which I would suggest you approach from its alphabetical site index at www.fema.gov/fema/. They include a Standard Checklist Criteria for Business Recovery, an Emergency Management Guide for Business and Industry, a Disaster Services - Disaster Supplies Kit (which lists everything from sun screen and toilet paper to family documents you should be prepared to carry away quickly from a disaster site) and a nice Financial Disaster Preparedness article (which includes sections on reviewing your insurance coverage for a home office, as well as other types of coverage available). It has a helpful section on creation of an “Evacuation Box,” which I highly recommend. Although that section, as written, is more helpful for residential use, an easy extrapolation would be one from including irreplaceable personal photographs , your will, and duplicate prescription insurance cards to backups of computer records, a supply of checks, employee data and key contacts information. I actually recommend such a box in my estate planning practice. If nothing else, it can be helpful to have an inexpensive fireproof box in which the above items are stored, as well as birth certificates, insurance policies, an inventory of the physical location, supporting documentation for making a claim, such as serial number and copies of purchase receipt for major items like appliances, cameras, jewelry, etc. This could also be a good place to place a copy of your funeral instructions and similar information, since it may be more likely to survive than you. Aside from locating the cat under the bed, this should speed up

your departure from a building in a crisis.

- Another useful site is www.riskinfo.com, which features links to some articles and vendors in the area of practical risk management.
- www.disasterplan.com has a handy “Disaster Recovery Yellow Pages™” section. It also has a one page Preparing for the Disaster-Recovery / Business-Continuation Plan document which could be amazing helpful. The sage advice in that article leads me to the close of this one.
“Remember, a disaster plan is never a fixed finished document - it evolves and gets better as time goes by. Therefore, it doesn’t have to be perfect the first time you do it - the important thing is to get started on it! Be systematic in your plan - don’t try to outguess Nature and plan for a flood, a hurricane, a fire, etc. Instead, look at the common elements in any disaster:

- ✓ loss of information
- ✓ loss of access to information & facilities
- ✓ loss of people.”

A few final thoughts:

- Prepare a grid or matrix of the essential functions of your business. In successive columns following each function, place the physical resources, communications links, documents, tools, and key personnel currently associated with each function. To the right of that, put the alternate method and resources which should be applied in the event of loss of the primary level resources, including total loss of facilities and primary personnel.
- Determine the location and advise your employees of the site of an emergency meeting place at least within walking distance of your facility. In the event of a “moderate” crisis, such as fire, sewer collapse, robbery, etc. this would be a place where everyone should be safe and could “meet up” to decide what to do next. A secondary “getaway” should similarly be determined, in the event of a more widespread crisis, such as a flood, airline crash, etc.
- Make clear what the crisis succession plan or chain of command, for each job function, would be in the event of death, disability or forced absence. (Did I say kidnaping?)
- Rehearse an evacuation or “hard reboot” of your company in the event your primary facility was destroyed or suffered major damage. Have each employee walk through how they would perform at least the most essential functions of their jobs from a remote location or take over for someone who was no longer present.
- Walk through the steps in totally (to the extent possible) restoring your business after a disaster. What alternate resources would be necessary? How would they be obtained and by whom, in the event of a tragedy? What could be done now or mapped out for the near future to speed up or reduce the cost of the company “reboot?”

- **Actually test the backups of all your software applications and data to see if they will work when restored.**
- **Go to your alternate emergency office. Walk through each essential function of your business. You may have a laptop at home with copies of data backups from your office, but do you have the program to restore and run from that location? Do you have a way to quickly access funds to buy replacement equipment or pay employees? Could you reach everyone at home or on the road if you were in your alternate location? Could you quickly reach customers, vendors and others who are critical to your company? Do you have contact information for those who you would need to assist you in restoring your company or replacing an employee. Do you and everyone else in your company have a current phone tree?**
- **Do you have passwords for software programs or Web site maintenance (perhaps the best way to get news out about your alternate business functions and company status would be the Web.)**

“Those who cannot remember the past are condemned to repeat it.” George Santayana

© 2001 by Stuart Adams. This is the 20th installment in the Author’s online book. Your comments and input would be appreciated in helping the Author make this an "organic book," which will continue to grow and adapt to change, just as any business itself must do. E-mail your comments and suggestions to the author at biz-law@juristechnology.com.