PRACTICELINK

CBA.ORG

SURVIVING CHAOS IN TIMES OF CRISIS:

Disaster recovery for small and medium-sized law practices

By Robert Patzelt

December 2003
Canadian Bar Association

About the author

Robert Patzelt is the Past-President of the Nova Scotia Canadian Bar Association and was the CBA's national Treasurer. In addition to this volunteer activity he is the past Chair of the Canadian Manufacturers and Exporters and past-Chair of their environment committee and was the industry representative on the Minister's Task Force on Contaminated Site Management for Nova Scotia. He is also on the national board of the CME and sits on its Executive Committee. Also, he is a Scout leader for First Clayton Park Scout Troop and is the past provincial President for Scouts in Nova Scotia and presently sits on the Board of Governors for Scouts Canada and is a member of their Audit Committee. In 2002 received the Queen's Golden Jubilee Medal for his contribution to Scouting.

During the day he is General Counsel and Group Risk Manager and a member of the executive team for Scotia Investments Limited a diversified holding company operating in 6 provinces in Canada and in one state with over 1500 employees. Activities include pulp & paper, food processing, transportation, floral production and real estate development. Robert has written papers and spoken to groups all over North America on a variety of legal and risk management issues including directors & officer's liability, risk management, insurance, institutional sexual abuse, the environment and assorted topics of an educational and motivational nature. He has spoken to such groups as the Nova Scotia Insurance Women's Association, Risk & Insurance Management Society, the Nova Scotia Barristers' Society, The Canadian Bar Association, Insurance Brokers Association of Newfoundland, Canadian Insurance Congress, Purchasing Managers Association of Canada (NS), Society of Risk Management Consultants, Technical University of Nova Scotia, Canadian and Nova Scotia School Board Association and the Association of Records Managers and Administrators.

He also has his Fellowship in the Insurance Institute of Canada and is a recipient of the Don Stuart Award, which is the highest Canadian designation, awarded to a person recognising their outstanding contributions to risk management.

He completed his Masters in Law with a thesis on Directors & Officers liability in 1996 from Dalhousie University. He has an undergraduate degree in Commerce (Accounting) from the University of Alberta as well as an Arts degree (Economics/Psychology) from the same university where he graduated with distinction as a member of the Dean's List. In 1998 Robert brought home to Nova Scotia the Insurance Institute of Canada's top award in Canada for public speaking. Most recently, Robert was involved in Tall Ships 2000, the largest tourism event in Atlantic Canadian history. He is a member of the Board of Directors and Executive of Tall Ships Nova Scotia and was the Chair of the Tall Ships 2000 Events and Marketing Committee, which was responsible for such activities as the management of the events, their promotion, and public relations.

Robert grew up in British Columbia where his parents still live on the family farm and has had a number of jobs including farmer, a member of the RCMP, schoolteacher, payroll clerk and was even in the accounting department of the Calgary Zoo. He has travelled to every province and territory of Canada and travelled extensively in Europe. Robert lives in Halifax with his wife Tracy, who is an actuary, and their four children aged between 13 and 8. As a result of his corporate duties, volunteer activities and his family commitments he has no free time but if there is some his family tries to go camping, weather permitting.

SURVIVING CHAOS IN TIMES OF CRISIS

Disaster recovery for small and medium-sized law practices
(however, this applies to the big firms too!)

TABLE OF CONTENTS

Introduction and Disclaimer

Disaster Recovery

The Disaster Recovery Plan

- Introduction
- Purpose of planning
- The disaster recovery plan itself
- Required thinking processes for disaster planning
- Producing the disaster recovery plan
- Training and testing: the key to success

Disaster Recovery Files

Risk Assessment

Pre-Loss Planning – What to do before a disaster

- Insurance
- Physical protection
- Security
- Earthquake
- Advance notice

Computer Protection

Coping with Disaster

- Signs that a person may need stress counseling or assistance
- Employee support
- Don’t forget about the children

Dealing with Insurers

Salvage from Water Damage

Conclusion

Appendices:

Possible Events and Hazard Checklist

Human including criminal activity
Natural disasters
Infrastructure disasters
Accidents involving other events

Emergency Contact List

Computer Inventory

SURVIVING CHAOS IN TIMES OF CRISIS

Disaster recovery for small and medium-sized law practices
(however, this applies to the big firms too!)

***"Life is what happens to you while you're busy making other plans."* John Lennon**

INTRODUCTION

In this day and age, planning for the unthinkable has become a requirement for any responsible business or enterprise and the practice of law is no different. As lawyers, we are called upon to assist our clients in their times of distress and difficulty, but are we ourselves in a position to deal with adversity if the practice were subject to an event or series of events that impaired its ability to continue normal activities?

This resource is provided to members of the CBA so that they are in a better position to react to disaster. Disasters can range from inconvenient computing problems to the complete destruction of your office.

dis·as·ter 1. a calamitous event, esp. one occurring suddenly and causing great damage or hardship. *

Re·cov·er·y 1. the act of recovering. 2. the possibility of recovering. 3. the regaining of something lost or taken away. 4. restoration or return to health or a normal condition, as after sickness or disaster. *

- The Random House College Dictionary, Revised Edition, Random House Inc. New York

DISCLAIMERS

This information includes data, commentary, checklists and tables, which are intended to minimize the damage and negative consequences resulting from loss especially those that could result in practice interruptions. This is not a complete analysis of any of the topics

covered and readers should conduct their own research and analysis, operational, legal or otherwise.

© 2003, Sanddollar Analytics Inc. All rights reserved. This resource has been provided to the Canadian Bar Association (CBA) under license only by CBA members to view, download and copy for use in their own practices. No part of this resource may be transcribed, reproduced, stored in any retrieval system or translated into any language or computer language in any form or by any means, mechanical, electronic, magnetic, optical, manual or otherwise without the prior written consent of Sanddollar Analytics Inc. Requests for consent may be directed through the CBA.

DISASTER RECOVERY

This document was written in 2003, during which Canadians found themselves at the mercy of a number of significant events including an outbreak of SARS, a massive power blackout, destructive forest fires in western Canada and a hurricane in eastern Canada. All of these events occurred within less than a year and all served to underline the point that we can no longer assume that things will always operate under the scenario of "business as usual". A negative event can occur at anytime and in many cases without warning.

In 2001, the United States was subjected to the most devastating terrorist attack in its history, the impacts of which are still being felt to this day. The New York Bar Association estimates that thousands of lawyers were displaced as a result of the destruction of the World Trade Center in New York City.

Aside from the terrible human tragedy, the events of that fateful day had the impact of refocusing disaster recovery efforts which were primarily concerned with information technology issues and forced them to concentrate on business continuity issues, such as how to communicate, how to stay in business and how to quickly get back to "business as usual". Some of the lessons learned were:

- Key personnel may not be available
- Communication, especially telephone, Internet and fax, is essential. See "**EMERGENCY CONTACT LIST**".
- Disaster recovery plans are absolutely critical and they have to be updated, tested and stored off site
- Vulnerabilities, strengths and dependencies must be properly analyzed
- Employees are key, and so too is having a communication strategy and plan to ensure that they are supported. See "**COPING WITH THE DISASTER"** for more information on supporting each other during very stressful periods.

Many people operate under the belief that a crisis will only happen to others. Others believe that their organization has unique characteristics that somehow make it immune to negative consequences. For example, they may feel that their organizations are too small to be affected in any significant way. In fact, the opposite may be true. Smaller organizations may lack the momentum or have few redundancies that allow organizations to cope during times of intense pressure.

Disasters like the terrorist attacks on the World Trade Center and the August 2003 power blackout inevitably grab headlines and capture our attention, but the majority of disasters are "quiet catastrophes" such as the failure of a computing system or the loss of a key employee. Are you prepared for these kinds of events?

What are the consequences of a significant computing failure to your firm? It is estimated that 45 per cent of all computer data losses are due to electrical power surges and power outages. Computing and telecommunications systems are subject to an average of 120 power problems per month. During a disaster there is a marked increase in telephone usage that may be simultaneously accompanied by a loss of telecommunications capacity, potentially disrupting normal operations. What's more, computers are prone to threats from other sources, including hardware failures, software errors, viruses and hackers, not to mention outright theft. See "**DATA RISKS**".

What if there is a fire and your office is seriously damaged or destroyed. Can you get the insurance process quickly and efficiently started? Are you able to continue to do billing and continue working? The majority of fires take place in non-working business hours (data show that 70 per cent of office fires occur between 9 p.m. and 9 a.m.) when people are not around to sound the alarm, call the fire department or extinguish the fire.
When addressing disasters and their consequences, the most important consideration is that one recognizes that disasters come in all forms and no one is immune. For a more complete list, see "**POSSIBLE EVENTS AND HAZARDS CHECKLIST**". Having said that, a proactive approach to disaster planning can accomplish much towards preventing negative events, minimizing their impact and returning to normal as quickly and as efficiently as possible.

THE DISASTER RECOVERY PLAN

INTRODUCTION

Planning for disaster and disaster recovery ensures that critical services and products are available during and after a disruptive event, allowing the firm to recover its facility, data and assets more quickly. Key elements of this process include the identification of key resources necessary to allow for business continuation including personnel, equipment, information and data and other organizational infrastructure requirements (also called business continuity planning). Disaster recovery planning should be a proactive process that includes:

- actions to be taken
- resources to be used; and
- procedures to be followed.

PURPOSE OF PLANNING

In short, you are trying to:

- Reduce risk of loss. A natural focus for a law firm will be on physical premises, computing equipment, communication equipment (especially telephone, fax and Internet), client files and documents, accounting and financial matters.
- Provide cost-effective ways of addressing risk. This will dovetail with insurance coverage and, in the long term, reduce cost of insurance.
- Ensure rapid and orderly recovery (avoid panic). Communication is critical to reassure employees and clients, control rumors, and manage the media. If you are in control and in a position to lead, your employees, clients and others will be reassured and will support you during these very difficult times.

THE DISASTER RECOVERY PLAN ITSELF

A disaster recovery plan includes alternatives to conducting business and is divided into three chronological parts:

- *Response to the event*
    - assume control
        - contact emergency services, if required (fire, ambulance, police, etc.)

- have a plan for notification of personnel and other key parties, such as clients, insurer and suppliers
    - advise your staff as to when and where you will need them
    - contact clients to the review situation, discuss files, etc.
    - contact suppliers
    - start the insurance claims process
    - redirect mail, telephone, etc.

TIP: *One of the key aspects of quick recovery is quick, effective communication. Consider alternate methods such as cell phones or back-up systems that will re-route existing telephone lines. Keep in mind that in a major power failure, the ability to use a fax, telephone or the Internet may be severely impaired.*

TIP: *Have as part of your plan an emergency contact list. This is a list of key resource people to call in the event of a disaster. See* "**EMERGENCY CONTACT LIST**".

- Identify the damage and its potential impact
- Implement the plan and coordinate resources

- *Continuation of critical services*

    - During the continuation phase, the plan will help ensure that critical services are delivered or that their interruption is minimized
    - Things to consider may include:
        - banking
        - payroll
        - office space and furnishings
        - equipment: computer, printer, fax, copier, etc.
        - office supplies: business supplies, stationary and business cards, etc.

- *Recovery and restoration*

    - During the recovery phase you will be focusing on getting back to "business as usual". This includes:

        - repair and rebuilding
        - redeploying personnel
        - acquiring needed resources to establish "normal" operations

REQUIRED THINKING PROCESSES FOR DISASTER PLANNING

Plan for the worst while hoping for the best. Pessimism is a key element of any disaster plan. Assume the worst possible scenarios and plan for them accordingly. Some "what if" questions to consider include:

- What if our key documents were destroyed in a fire?
- What if we could not gain access to our building for an extended period of time?
- What if we had someone (or many people) injured or killed?
- What if our computer systems went down?
- What if our clients could not contact us?

Worst-case scenario development is a useful tool and by planning for the worst, lower impact events can be addressed more easily. A worst-case scenario is something that completely stops you from carrying on your practice. A fire that totally destroys your office is a good example.

What functions and people are essential? To properly develop your disaster recovery plan you will need to consider who in your organization does what, when and where? Analyze your practice processes and estimate how long it will take to get certain aspects operational again. For example, access to your docket and calendar may be immediately more critical than, say, payroll services. A small organization may simply cut cheques as an advance close to the amounts employees normally would receive and make payroll adjustments at a later date. Getting alternate office space may be harder than replacing lost computers. Then again, a one or two-person firm could possibly continue operations out of their home, and in fact, may already have home computers that are fully compatible. On the other hand, if your office and home are in the same location and it is destroyed, your situation is even more dire. You have the added burden of having to deal with your business and personal matters at the very same time.

Try and identify the hazards y+ou may face. Many examples have already been noted. You are looking for things that can happen to your people, your physical assets and your systems, which includes legal, financial and technical. Look at what can affect your facilities, your operations, and identify your critical elements of information and communication as well as pre-loss actions you can take such as insurance and prevention. In light of those hazards, what is their potential impact and how would you plan to keep the doors of your practice open? For a more complete list see **"POSSIBLE EVENTS AND HAZARD CHECKLIST".**

TIP: *Every plan is unique to each organization. Focus on those elements that you can reasonably control and do not get bogged down in excessive detail, such as concentrating on things that are outside your sphere of influence. For example, document your computer systems and their elements so that you can quickly repurchase a compatible system that meets your needs. You will not be required to have a list of all potential suppliers, however, the company that sold you your existing system is a good starting*

point. Keep things simple. This is a guide and a resource. No one can anticipate every negative event and plan for every circumstance and consequence. Also, it is not necessary to deal with every kind of calamity in great detail. The loss of an office whether by fire or flood has the same operational results. Prioritize by completing a risk analysis. See "**RISK ASSESSMENT**"

PRODUCING THE DISASTER PLAN

In preparation for producing your plan you should:

- Identify critical processes and recovery time frames. See "**DISASTER RECOVERY FILES**".

- Set priorities for the functions that make your practice run. They must be based on minimum requirements to achieve acceptable levels of service delivery and the maximum time you can be unable to operate before causing severe damage to your operations financially and to your reputation. This includes an analysis of loss of service delivery for extended periods. Other impacts include loss of revenue, additional expenses that may be incurred and intangible impacts like loss of reputation.

TIP: *If you have not already done so, establish a line of credit. This will provide you with the necessary operating capital to keep you afloat until practice operations and fees start to flow again. See* "**DISASTER RECOVERY FILES**" *for more helpful hints.*

- Define your minimum requirements. What can you possibly not live without? What can be obtained temporarily from someone or somewhere else?

- Protect as best as possible your minimum requirements that are cost-justifiable. Within each plan there are several possible courses of action, but some may be impractical or economically prohibitive. In larger organizations it is estimated that it can cost up to 3.5 times more than the basic system to have a fully operational and redundant network system. This is not practical for a small practice especially if key elements can temporarily be operated on a substitute basis. For example, a small firm may have the ability to perform manually what is done electronically. A large organization cannot do payroll manually but a small practice can or may already do so. Small firms do not have many (if any) IT staff on hand. They will not have many branches where work and resources can be redirected.

- Your plan must include written documentation for response, continuation and recovery.

TIP: *Keep your plan simple and easy-to-use. Put as much information and detail in appendices. Your plan should be divided into quick and simple sections. Use clear and plain language. This is a quick reference guide—not a piece of elegant prose.*

TRAINING AND TESTING: The Keys to Success

Test the plan and train employees. It is critical that employees know that the plan exists and how it works. An actual disaster is not the time to test the plan, however, recreating a mock disaster can be very expensive and complicated. However, elements can be tested at different times. For example, a "fan out" or "call out" can be tried out just to make sure your contact information is current and accurate. The fan out or call out is simply a communication cascading system. It is a process that allows persons to contact members of the firm in a manner as prescribed in the plan.

Paper-based exercises allow the group to read through and test elements the plan. Test each action and assess whether it is: the right thing to do, whether there is a better way to complete the action and whether the actions are being carried out in the proper sequence. You can test it against your previously developed "what if" or "worst case scenarios". Just like fire drills at school, you can perform a similar function for your business by practicing various elements such as restoring data from your backups.

TIP: *The purpose of a test is to avoid gaps and make improvements. If after completing your test no concerns or errors were detected, your review may not have been sufficiently aggressive. A complete test of the system should reveal a surprise or two.*

Even with a plan, there is much that can be done before the event. Two key elements address matters related to insurance. See "**PRE-LOSS - INSURANCE**". Also, there is much that can be done on the preventative side or in mitigation. See "**PRE-LOSS – PHYSICAL PROTECTION**".

TIP: *Remember, the documentation you are writing may not be for you. Be sure that it is clear as someone else may have to implement your plan, do data recovery, etc.*

DISASTER RECOVERY FILES

The purpose of this activity is to ensure key information is protected and preserved for your disaster recovery. In the event of a total failure, your firm's data files – important client listings and information – can be significantly more important and more difficult to retrieve than the physical systems that house them.

Produce two sets of backup tapes of computer data. Place one set in a secure, fire resistive cabinet in your office and a second copy off site. Be sure that the off site storage is located at a distance to ensure localized damage or destruction does not affect both sets of tapes.

Have a copy of all service contractors. Information should include: name, address, telephone numbers and contact person for all computer and key office equipment.

TIP: *Have a copy of every credit card and account number and 1 800 numbers in case your purse or wallet is lost or stolen. Do the same for bank accounts and store all of this in your secure location(s).*

Important data files to be preserved in disaster recovery files include:

- Client data: name, address, and file numbers for all open files. It is a good idea to have a client file index and off site file storage index. Conflict of interest and client/matter intake information is also very valuable.
- Docketing/calendar information for individual lawyers or a master for the firm. Be careful of items in personal digital assistants or in pocket calendars that are not on the system. They may be lost in the disaster. See "**CHECKLIST FOR BACKUPS**".
- Practice or partnership agreements and documents including minute book
- Clerks of the various courts and key court personnel contact information.
- Names, addresses and phone numbers, including cell phones and cottages, for the whole firm. Also, have voice mail and computer passwords. Special medical information may also be useful. Be sure that this information and other disaster recovery files are safely kept.
- Key information about partners including SIN, location of will, power of attorney or trust, safe deposit box (contents, signatory information, location of key).
- Business numbers (e.g. GST, HST, etc.)
- Business and financial accounts: names, address, phone numbers, account numbers and signatory information including payroll company. Payroll, benefits and other human resource information may also be valuable. Accounts payable, accounts receivable and other key financial information may also prove to be valuable.
- Names, addresses, phone numbers, policy numbers and contact for insurers and broker/agent for all insurance policies: property, errors and omissions, liability, valuable papers, health and disability and life.

- Emergency contact information (personal representative, doctor, accountant and others) for all lawyers and staff, including which relatives to call, and school and childcare information. For solo practitioners it is important that you have some backup lawyers who can be called upon to address or handle various legal situations or files in the event you become ill or injured.
- Registration and license number of all the firm's software including items preloaded on PCs.
- Serial or registration numbers on all office equipment (fax, scanners, telephone, dictation, etc.) and computer hardware; names, addresses and phone numbers of key suppliers and lessors; and account numbers and leases (including expiration date).
- List of all maintenance contracts and warranty information.
- List of all major purchases including date and purchase price (can be a simple electronic file or a file with receipts or invoices).
- List of all library contents and subscriptions.
- Petty cash and blank cheques. Continued payment on firm cheques sends a message of "business as usual". Also, consider withdrawing the maximum from your ATM or bank account. This provides cash flow in the event banking services are interrupted during this critical period.
- Consider having some things like letterhead, envelopes and business cards on hand at all times at an off site location. Just like quickly redirecting calls to a different location, paying your bills with your stash of cheques, the use of letterhead, etc. gives the impression that things remain under control.

There is a tendency to focus on electronic files or records and in many cases this makes a great deal of sense. It still is very important to ensure that your focus is not too limiting. Records are more than electronic and paper files. They include diaries, information on maps, plans, photographs, etc. Some of us in the process of moving to newer computer systems still maintain records in "older" forms such as in archived file cabinets and on older computers that are not compatible but are retained for those few times we need to access something.

RISK ASSESSMENT

As part of the disaster recovery process it is useful to plot a matrix of risks and their potential consequences. It is key in noting vulnerabilities. This need not be an elaborate and complicated process. In fact, the simpler the chart, the more useful. Noted below are a couple of examples. After having listed the risks and their probability and consequences, one can then turn their attention to preventative measures and the disaster plan itself.

Below is an example of a risk assessment table with a few examples.

Probability rating:

5 – very high
4 – high
3 – medium
2 – low
1 – very low

Impact rating:

5 – terminal
4 – devastating
3 – critical
2 – controllable
1 - irritating

Risk (event or consequence)	**Probability** (high to low) (5 to 1)	**Human Impact** (high to low) (5 to 1)	**Property Impact** (high to low) (5 to 1)	**Practice Impact** (high to low) (5 to 1)	**Internal Resources**	**External Resources**	**Preventative Measures**	
Death or serious injury to partner	2	5	N/A	4	Only two partners in the firm and she is responsible for most client work and specialty tax advice	Can get tax advice from other firms	- ensure clients comfortable with both partners to minimize loss, establish contacts in other areas of practice	

Theft of office computers	2 (except for laptops which would be a 4)	1	4	4	Other computers in the firm and old one at home Not sure if partners have all the same data	Can purchase a new computer quickly	- ensure computers in firm are all compatible - regular and complete backup of OS, software and files - plan should include vendor contact info	
Fire	1 – modern building, well protected,	4	5	5	Home offices	- lots of rental space available - office equipment can be purchased	- need proper insurance - proper backup systems - ensure home office is compatible	

TIP: *A little brainstorming is useful for this exercise. There are no right or wrong answers. Develop different scenarios and have a group discussion of all the different elements. The different perspectives will be very enlightening. In addition, all sorts of pre-loss ideas come to the fore.*

PRE-LOSS PLANNING
WHAT TO DO BEFORE A DISASTER

Much damage, and in many cases, a disaster itself can be avoided with a little pre-loss planning and a little luck. “Chance,” it is said, “favours a prepared mind”.

INSURANCE POLICY

Review your insurance policy on an annual basis. Many policy holders discover only after a loss that their policy does not adequately address all of their real losses. A lack of adequate or proper insurance could be financially devastating.

Review and discuss the following with your insurance advisor to ensure that your needs are properly met:

- Determine what perils or causes of loss are covered by your policy. Also consider issues such as replacement value versus actual cash value, all risk including flood and earthquake, sprinkler and water damage protection, cleaning and restoration costs, and payment of interim rent. These things may have to be added by a special endorsement or rider.
- Consider how your assets will be valued in the event of a loss.
- Consider deductibles, which levels are acceptable to you, and their impact on your insurance premiums.
- Determine how much insurance (to what values must you be insured) is required to avoid any surprise effects from co-insurance clauses.
- Consider an endorsement to cover the costs of required upgrades to meet existing codes.
- Ensure that you have coverage for other items, such as:
    - business interruption (how much and for how long) to cover for loss of income (if you own the building you may also be a landlord and will potentially may have a loss of rental income)
    - payment of interim rent
    - extra expense to cover extraordinary costs (temporary leasing of equipment, restoring lost data, additional temporary employees)
    - cleaning, restoration, demolition and debris removal
    - interruption by a civil authority
    - crime coverage
    - equipment breakdown
    - computers/electronic media
    - valuable documents including the cost to recreate files
    - disability, health and life insurance
- Consider what may be expected of you by your insurer in the event of a loss
- Consider the kind of records and documentation will you need to quickly and properly process your claim

- If you have a home office, consider having computers and other items covered by your homeowners' policy. Consider also the value of personal items left at the office.
- Consider insuring home, office, property and vehicles with the same carrier to avoid coverage gaps. Note that property insurance may not cover all perils, such as water damage or damage from snow or ice, if it is caused by the failure of the owner to remove the snow and ice or by a steam explosion (some buildings have hot water heating as a source).
- Consider an umbrella liability policy for a nominal premium to greatly increase the amount of coverage available for liability exposures.

PHYSICAL PROTECTION

Fire

Smoke and heat detectors are good risk management devices. Heat detectors are preferred, as a fire will produce heat before any appreciable increase in temperature results in smoke. If using a smoke detector, use a good quality ionization detector, as it will detect airborne invisible products before smoke becomes visible. Also, remember to check batteries frequently.

Have appropriate fire extinguishers that are visually inspected monthly and serviced annually. Also, it is very helpful if all staff is trained in their proper use.

Store flammables, such as cleaning solvents and other combustibles in an approved fire rated cabinets.

Restrict smoking to off-site or designated areas.

Flood and water damage

Two key methods to protect against water damage include, preventing the entry or escape of water and ensuring assets are located as far away as possible from potential sources of water damage.

Ensure the roof is well maintained and check for signs of water entry. Flat roofs are more vulnerable because water has a better chance of collection and seepage.

Avoid below ground storage and storage in areas near water and sewer pipes in the building,

Have your sprinkler system regular checked and maintained.

See "**SALVAGE FROM WATER DAMAGE**"

SECURITY

Clearly mark areas that are closed to the public and are for staff only. Visitors should be escorted in these areas.

Be sure reception areas are always staffed or have a way of restricting entry to private or secure areas.

Physical security includes ensuring:

- doors, windows, loading/receiving areas and other entry points are secure and locked at the appropriate times and at the end of each day. Do not lock or block emergency exits and fire escapes;

- access control systems and alarm systems are maintained on a regular basis and train staff and outside contractors (e.g. janitorial, etc.) as to their proper use;

- employees have a place to lock valuables (e.g. purses, laptops, etc.);

- employees who work late can safely make it to their automobiles or transit; and

- former employees turn in all keys, identification, access cards and make the appropriate changes to locks and access codes.

EARTHQUAKE

Primarily, the earthquake areas in Canada are on the west coast and in the St. Lawrence River area, but they can occur anywhere. There are actions that can be taken to minimize damage from an earthquake:

- anchor tall bookcase and filing cabinets to walls
- secure water heaters to walls
- brace racks, shelves and other items to prevent tipping
- attach computers and small appliances to desks with Velcro or similar material
- use latches to keep drawers and cabinets from opening
- use closed screw-eyes and wire to secure items, such as pictures and mirrors to the walls
- ensure staff knows where to find and how to shut of your utilities and, if allowed, install a breakaway gas shut-off device.

ADVANCE NOTICE

In some cases you maybe be fortunate enough to be forewarned of a potential disaster, such as a hurricane flood or interruption by a civil authrority. In those cases, you may be afforded the opportunity to protect yourself. Of course, safe evacuation is a key priority. Consult your disaster recovery plan, listen to the news, and take the following preventative actions:

- Backup your computer files and take as much computing data and equipment as time permits.
- Shut off all master power switches and gas lines. Be sure you and your staff know where your electrical breaker is and that it is properly labeled. For those that are tenants, you may or may not have the ability to cut off your own power supply, as it may be part of a larger system.
- Move valuables to a safe place preferably off site, but if not, in the interior of the building.
- Cover valuable assets that cannot be moved with heavy gauge plastic and wrap it as tightly and securely as you can.
- Secure loose objects and move them away from doorways, windows and glassed-in areas.
- Close doors to all rooms and secure windows to reduce the danger of flying glass and weather damage.
- Keep as much as you can off the floor.

TIP: *It cannot be overemphasized that an ounce of prevention is worth a pound of cure. A little pre-loss planning goes a long way toward minimizing the effects of a disaster. At worst, you feel a little more confident that you have done the most that you can. At best, you may avoid a major catastrophe or severely mitigate the negative circumstances of a disaster.*

COMPUTER PROTECTION

TIPS FOR COMPUTER SECURITY

The importance of backing up software and data files cannot be overstressed. Backup regularly and test backups to ensure that the data is retrievable. Replace backup media tapes annually (preferably every six months). There are a host of economical digital backup tapes and removable storage devices on the market. Make sure you test your backup. See "**CHECKLIST FOR BACKUPS**". You need to develop a healthy distrust of the integrity of your system. Remember that computer systems are prone to failure.

One of the problems with backup systems is they are becoming obsolete as quickly as other computing products. Older backup systems frequently do not backup open files, which you must consider as many e-mail and case management programs or databases are generally open all the time. There are companies that specialize in recovery of data from obsolete tapes and equipment or damaged hard drives. Consider a duplicate PC or server with identical software and backup capabilities to be located away from the office. This may be a practical solution for practitioners that have both office and home office locations.

TIP: *Make copies of your key software on CDs. Store them off site with serial/license/registration numbers. You will need a CD-writer, which are becoming more affordable and more commonplace on newer computers.*

Consider "document mirroring" or "document shadowing" software where every time you save a document to the Windows folder a copy is also stored in the hard drive. If you experience a server failure, you may be able to access the last 90 days of documents previously saved.

Also consider "case management synchronization or replication" technology. A lot of case management software allows access to dockets and case information when a lawyer is mobile but it also synchronizes everyday so that multiple PCs have the same information. If there is a network failure, more than one PC has access to critical data. Once the server is back up and running, you simply resynchronize much in the same way you can synchronize your PDA with your PC.

Virus protection is a critical risk management tool. Purchase virus protection and subscribe to an online update service. New viruses are constantly being created and you need to ensure that this protective measure is as current as can be.

Internet users should install a firewall, test it regularly and plug detected leaks. As a side benefit, it will also reduce all sorts of those pesky pop-ups that you may receive.

Develop and follow a records retention policy. Have a process for determining the deletion of files. Also, such a process will help get rid of old and embarrassing emails.

Protect system passwords by changing them on a regular basis—moving targets are much harder to hit. Do not give remote access passwords to anyone else, even within the firm, and do not make passwords guessable (for example, your own name, or the firm's name). Above all, do not post passwords where they can easily be found. Some people keep their passwords in their wallets or purses, at their desk or posted on the wall. Believe it or not, most hackers do not use hi-tech means to gain access. They will call for them or go through the trash. With the use of remote access the integrity of the password becomes more critical. Consider encryption as an added protection.

Develop security policies and procedures and regularly audit compliance. If you are a sole practitioner or in a very small firm, make sure you exercise the discipline the same way a larger firm would, such as regularly changing passwords, etc. Your exposure is equal and your vulnerability may even be greater.

CHECKLIST FOR BACKUPS

The people process:

1) Who is assigned to do backups? Ensure that this task is assigned to a specific individual including someone as an alternative to cover when the primary person is away on vacation, sick days, etc.

2) Create a set of protocols. Ensure that you have written policies as to how backups are to be conducted (see the how-to process below). It is best to conduct backups at the same time each day to develop a habit of completing them. Some programs allow for backups to be done during off hours. Depending on the size of the backup, the process can take between minutes and hours. The point of a backup is to be able to restore current data. Ensure that you have written policies for how to restore data and ensure that several people are properly trained.

   TIP: *You are not writing a system backup document for yourself, but for someone who may not be familiar or trained on your computing system.*

3) Have a policy that ensures that there is a written log of all backups. Most backup programs automatically create a log report. Review the log report periodically to ensure the backup was fully completed and that there were no problems.

4) Test your system and backup. There is only one way to test the integrity of your backup—do a full restoration. This ensures not only that the backup is complete and that the equipment is compatible, but that the process itself is sound. Record the qualities of your computing system so you can find a similar system. Remember, your computer system may be damaged or destroyed and you will need to restore the data on some other equipment.

5) Test your backup systems on a compatible computer system to further ensure the integrity of the process. There are a few things that one should focus on to ensure a successful backup:

- Is there adequate disk space and configuration to hold your backup database? The server level settings may need to be identical in order to complete a successful restoration.
- Are the user usernames and passwords on your server synchronized with those on the server on which you are performing the restoration? Frequently there are two records for a user—one at the server level and one at the database level.
- What are the requirements to point your users to a different server?

The physical process:

6) Conduct backups every day. Completing a full backup on a daily basis ensures that your data is as complete as possible and ensures that at worst the firm loses a day's worth of work.

7) Make sure you are doing a **COMPLETE** backup. This includes software and data.
   - Backup everything, not just what is on the server. Include data on laptops, individual computers (including the ones at home) and on other equipment such as PDAs.
   - Make sure open files are backed up. Many e-mail, database files and accounting systems are open all the time. Files that are in use may also be open and may not be backed up. Older backup software may not backup open files.

The physical equipment:

8) Rotate your tapes regularly, and do not use the same tape over and over. Use a series of tapes and use the oldest tape to do the latest backup. The advantage of doing regular and daily backups is that if you suffer from some sort of data corruption, you have the potential of going back in time to the point just before the problem occurred.

TIP: *Only bring with you the tape on which you are about to do the backup. All others must remain in their offsite storage place. You do not want to have all of your backup tapes in the same location as the data being backed up.*

9) Replace tapes regularly. Time and use are the enemies of any piece of equipment and backup tapes are no exception. Generally, tapes should be replaced every six months. You can use these tapes for larger backups like an

end of month or end of year backup. Consider changing tapes with the change of daylight savings time. It is a good reminder mechanism.

And finally, the most important thing (besides doing a backup):

10) Ensure you have off site storage for your backup tapes and your written policies. Although it is good practice to backup between computers or servers within the same office, it will do you no good if the tape is sitting in a desk that was destroyed by the same event that destroyed the rest of the office. Also, you need not only the data but also the procedures as to how to restore your files.

DATA RISKS

Computers have become overwhelmingly prevalent in the modern practice of law. Important as they are, however, computers are not immune to threats, many of which come not from outside sources like viruses or physical damage, but from internal ones like system failures. A hard disk failure, for example, is one of the most disconcerting and commonly held concerns of computer users. Other threats to data files include:

Software failure – Poor software design or computer bugs can cause the loss of data. For example, when saving a file some software may remove an old file before the new one is "saved" as opposed to creating a temporary file and then renaming it to the correct file name once the save is properly completed. If in the former you have a crash upon saving the file, both the new and old file may be lost.

Viruses – Viruses are malicious programs that can cause all sorts of damage including the loss of data and even program damage from the efforts to remove the virus. See "**VIRUSES**".

Human error – One of the most common mistakes made by the operator is accidental deletion of a file or files. Different mechanisms may be in place to prevent such events, such as pop-up reminders and "undeletion" utilities. However, you can still make mistakes such as saving over an existing file, or losing a file while renaming. One tip is to slightly change the name of subsequent drafts, e.g. <clientletter-dr1.doc> and the second draft would be <clientletter-dr2.doc>. Also, your daily backup may be a lifesaver from this kind of error.

File system corruption – There are numerous ways that the file system containing programs and data on a hard disk can become damaged or corrupted. Proper maintenance and regular scanning of the file system is a good preventative measure.

Hardware failure – Your hard disk is the primary repository for your programs and data and, as a result, a failure can be a very debilitating event. This reinforces the need for daily backups. Power losses at the wrong time (such as when you are doing sensitive operations on your hard disk) can result in the loss of many files. There are other causes

of data loss such as memory errors, etc. You don't need to be a computer expert to understand the impacts such losses could have—just acknowledge that your programs and data are at risk and ensure the best preventative measures are implemented.

TIP: *Purchase surge protection devices for all your computer and telephone equipment. A surge protector with a battery backup will assist in keeping things operational during power losses, even if it is only for a period of time long enough to conduct a proper shutdown and maybe even a backup. A power surge through the telephone line has the capability to destroy a computer through the connected modem.*

Human evils – Theft and sabotage are unfortunate realities. Your office can be broken into or your laptop may be stolen from you at the airport. A disgruntled employee can do a lot of damage. Backups will not prevent theft or sabotage but it does make the possibility of adequate restoration a major protection.

VIRUSES

What is a virus?

A computer virus is a malicious program designed, in its most innocuous form, to be a nuisance and to cause irreparable harm at its most invasive. Viruses can be hidden in any program, be it contained on CDs, floppy disks, in e-mail attachments or downloaded from the Internet.

Once a virus has managed to get into your system, it can copy itself onto other files and disks accessed by the user. There are three main kinds of viruses: macro, boot and parasitic.

Macro viruses automatically carry out program commands. They will self-replicate. If you access a document that contains a macro virus and the macro is executed, the computer becomes infected and any document on your computer that uses this application becomes infected. If you are tied to a network the infection can spread rapidly. This is the most common type of virus and the inherent reason for its ability to spread is because of the high rate of exchange between parties.

Parasitic viruses are attached to programs (also referred to as "executables") and when you launch your program, the virus launches. Your operating system is lead to believe that the virus is part of the program and allows it access to the program where it can replicate, install itself into memory or release its evil payload.

Boot sector viruses modify the contents of the boot sector program. The boot sector is the first software loaded on your computer and the virus replaces your original boot sector program with its own "modified" content.

Virus Protection

There are a few measures you can take to protect yourself:

- Make backups of all software, operating systems and files. If you are infected with a virus you will be able to perform a restoration of your system.
- Use anti-virus software and update the software regularly. This allows your system to detect, report and in some cases destroy viruses.
- Be careful as to where you get programs, data, etc. As indicated, the ability to be infected increases greatly as people share information. Be mindful as to the source of your information:
    - be careful on what you download from the Web
    - open email attachments with caution. Do not open attachments from sources you do not know
    - be careful of what you have received from others on floppy disks, etc.
- Consider installing a firewall.

COPING WITH DISASTER

The peripheral pressures associated with dealing with a disaster can often be as destructive as the disaster itself. Consider not only the effects of a disaster on your office's physical systems, but also on staff and their immediate families. It is perfectly normal to feel anxious and concern for not only your own safety and well being but for the safety and well being of others.

There are a number of things you can do.

1) Do not blame yourself for the event. Recognize that you will be frustrated at different times by your inability to control things around you.

2) Maintain as closely as possible a normal routine for your household and work. Try and limit demands that are not directly related to your goal of restoring normality to you, your business and family.

3) Even if you find it difficult, try and talk about your feelings with someone. Anger, sorrow and grief are normal reactions.

4) Seek assistance from others, including other lawyers and professional counselors. The Legal Profession Assistance Conference (LPAC) is a great resource. Also, focus on your respective strengths and abilities.

Signs that a person may need stress counseling or assistance:

- The emotional roller coaster – easily frustrated, mood swings, crying easily, overwhelming guilt and self doubt, depression, sadness, feelings of hopelessness, new fears (e.g. not wanting to leave house, fear of crowds, etc.).

- Health symptoms – headaches, stomach pains, colds or flu-like symptoms, tunnel vision and muffled hearing.

- Other – difficulty sleeping, difficulty communication thoughts, confusion, disorientation, difficulty concentrating and limited attention span, increased use of drugs or alcohol, poor work performance and difficulty maintaining balance in life.

Employee support

Employees will rely on you for leadership and support. Especially in a disaster that affects many people in the same region, they will not only share in their concern for the practice but they will have the same concerns for the issues that are affecting them personally. You may want to consider:

- cash advances
- salary continuation
- reduced or flexible work hours
- care packages
- counseling
- daycare or babysitting support

Don’t forget about the children

Children react differently to disasters than adults. They need not be directly exposed but can be affected by seeing an event on television or more likely by overhearing adults discussing the event. Children can react at anytime with feelings of fear, confusion and insecurity.

It is very important to answer their questions honestly. They will need lots of encouragement. Limit discussion of overly graphic details and ensure that you do not damage their perception of their safety. They will internalize some of your anxieties, such as your concern about financial matters. Try and maintain a normal home and school routine and continue to participate in recreational activities. Temporarily reduce your expectations about school and even substitute less demanding household chores.

DEALING WITH INSURERS

Notify the insurers

Notify of loss and get advice as to emergency repairs and expenditures. Ask if they will pay for living expenses (hotel, laundry, etc.) if you are unable to live and work in your home and see if such payments reduce the limit in your policy that affects payment for damages to property and business interruption.

TIP: *It may be very appropriate to notify your law society and E&O insurer to inform them of the disaster and to obtain counsel regarding how to avoid any problems associated with a claim for malpractice (e.g. a missed deadline).*

Making the claim

Keep records of temporary repairs to prevent further damage and items partially damaged. Keep all receipts, even if you are unsure as to whether the expense is eligible (you may still need the receipt for tax or accounting purposes, even if it is not applicable to an insurance claim). It is better to discard a receipt later than to not have the documentation in the first place.

In the event you are making a claim for business interruption based on interruption by a civil authority, keep a record of communications regarding evacuation orders including who made the order along with the date and time. An example of an interruption by a civil authority is being ordered out of an area by the fire chief or the police in the event of a chemical spill. You may not receive a formal or written order to evacuate and in many cases it is a recommendation to leave. The more and better information, the increased likelihood your claim under this section of your policy will not be denied. Compare information with others similarly affected.

Make a list of damaged property (photos and videos are a good idea) and check against your pre-disaster list. If you do not have a list, check with employees and partners and use other sources of information to jog the memory (e.g. view old photos, visit someone else's office with similar surroundings and resources, do a floor plan, go to office supply companies, etc.). You will be surprised at how many items you will miss on your first go through.

TIP: *It is a very good idea to videotape all office equipment every six months and immediately after a major purchase, renovation or move. Videotape the contents of all drawers, cabinets, storage areas, desks and do not forget those low traffic areas like storage closets, back rooms, etc. You would be surprised how many staplers, briefcases, etc. you own and you may forget about miscellaneous pieces of software. Store the tape(s) off site.*

Collect all the information that will assist in proving the value of destroyed or damaged property. Consider secondary sources such as invoices, bills of sale, receipts, and credit card statements.

Reconstruct lost records

If you do not have a full and complete backup of all your information, you may need to reconstruct for lost or missing information. This may include:

- Banking records: go to your bank, bookkeeper or accountant. You are looking for cheques, online transactions, deposits, statements, borrowing documentation.

- Information on clients and suppliers: statements, receipts, orders, invoices

- Tax department: latest filings and rulings

Notification

It is very important to advise staff ASAP—this is a key step in keeping control. If you are leading they will follow. Accept the fact that you will have to stall some for a while.

Contact clients and suppliers and explain your situation. You will be able (depending on the situation) to maintain most if not all commitments albeit some will have to be revised.

Notify your creditors as to payment delays, lost bills, etc. Try to negotiate new payment dates or reduction or delay in charges or penalties.

Notify your utilities to ensure service is restored as soon as possible, especially if your location is unusable in which case payments should be discontinued.

Filing insurance claims

Gather all policy information (numbers and company contact information). Use your insurance agent or broker. The burden rests with you in making your claim. It requires good and accurate information and documentation.

Discuss with the adjuster how the claim will be handled. Ask for interim payments. File an interim proof of loss. On widespread disasters there may be special procedures for addressing the situation. In some cases insurers will, upon receiving proof you are an insured, immediately issue cheques for a certain percentage of the insured amount to assist in the claims process.

Key questions you may have for your adjuster or insurance representative may include:

- Confirmation of the coverage you have

- Confirmation as to the appropriateness of repairs and clean up you have or are about to undertake
- Concerns about resumption of operations
    - What expenses are covered in moving to another location
    - Coverage for loss of income if you had to cease operations because of a civil order
    - Coverage even if you did not suffer a direct physical loss or property damage but you have lost income

TIP: *File your claim ASAP to minimize cash flow issues. You may be under increased financial pressure as you may still be paying bills while your ability to earn fees or bill for them has been reduced. Many insurers are also willing to provide partial payments in advance of final settlement.*

Help adjusters help you. Provide quick and easy access to you and your information. Clear communication and understanding is important. Provide a preliminary estimate of damages and costs including an estimate of the time you expect to be fully recovered. Help them set up an adequate reserve for your claim. This is especially true regarding making a business interruption claim.

- Make a preliminary list of the steps you are going to take to resume your practice on a full or partial basis. Your written disaster recovery plan will be of great assistance and providing a copy to your adjuster will not only impress them but will assist greatly in the claims process as they will see they are dealing with a prepared and sophisticated person.
- Consider all of your financial needs including payroll and debt obligations that will affect you during your recovery period.
- Keep excellent records of extra expenses. These are expenses that are incurred to expedite the return or rebuilding of your practice. This may include:
    - Temporarily renting replacement equipment
    - Operational expenses at another location
    - Moving expenses
    - Special charges for moving telephone lines, etc.

As a general rule, business interruption is an estimate of your loss of business income based primarily on historical records. One must be very mindful that your loss estimate is a reasonable one. Some practice revenues are not easily calculated. For example, if a large portion of your fees comes from contingency this results in revenues being less regular than, say, that of a wills and estates practitioner. Good sources of information could include:

- Past financial statements – keep a close eye on your expenses as they tend to be more consistent from period to period
- Income tax forms
- Other practice records, billings, expenses, credit cards, banking information.

Take notes of all conversations. Confirm discussions and agreements by following up in writing. Compare your experiences and notes with similarly affected people.

Use your information, pre-loss and post-loss to ensure the settlement is fair and reasonable. If it is not, discuss this with the adjuster. If the amount offered is still unsatisfactory, file an appeal and take the appropriate procedures to keep the right to future claims and payments open.

Discuss with your financial advisor any special treatment you may be entitled to in dealing with losses.

Beware of decisions made in the heat of battle.

Deal with reputable contractors with Workers' Compensation coverage and liability insurance. Try to avoid making bad decisions because of your desire to rush to get things done. Get estimates from more than one contractor and get contracts in writing.

Try and match payments with timing of insurance proceeds. Make sure final payment is not required until the job is finished. If you have suffered a loss that has also affected many in your area, such as a flood, you may have added challenges in getting contractors and other services.

SALVAGE FROM WATER DAMAGE

Water damage is a frequently occurring event, be it as a result of rain, flooding or pipe damage. The reason for focusing on its effects here is because water damage is a preventable occurrence, the damage from which can often be mitigated.

The most common sources of water damage are sprinklers, flooding and storms. Frequently this is one of those "quiet catastrophes". Generally, water damage is very messy and may require a lot of labour to address. Compounding the problem is future damage from mould and mould spores, which grow quickly in proper conditions and are highly toxic.

One of the first steps to mitigating water damage is to dry out the building. You are fighting an uphill battle if you are trying to dry out objects when the structure is still wet. Here are some tips:

- Remove as much from the building as practical, such as curtains, stationary, etc. You may need to remove the carpet. Check the underlay as it acts as a giant sponge.
- Find areas where water has the opportunity to gather, such as behind shelves, under furniture and in backrooms and closets. Work with your wettest items first.
- Get the air circulating. Open windows and install fans and dehumidifiers. You can use cardboard to build simple wind tunnels to direct the flow of air to where you want it directed. Try and maintain the temperature 10C to 15C with a humidity level of 25 to 33 per cent. Do not add heat until dehumidification and circulation is complete.
- Cover surfaces you wish to dry with absorbent paper, and change it regularly.

Air Drying

When air-drying books, try and remove plastic covers and insert paper towel in regular intervals (but not all the way to the spine) within the book and stand it up with the wettest end up. If it will not stand, let it lie flat. Do not interleave every page, as this will cause the book of the spine to swell and create permanent damage. Change the paper towel regularly. Many legal texts have thick covers. In this case, place a water-resistant film to prevent moisture from migrating to inner pages. You may hang books, papers, magazines and photographs from a line unless heavily sodden.

TIP: *As a general rule, if you cannot dry something out within 48 hours—freeze it.*

Freezing will preserve paper up to six years. Commercial blast freezers are best as they have lots of capacity and can drop temperatures quickly. A household chest type freezer with a temperature of -10 C is adequate for a small amount of material. Unless extremely wet, most paper-based items will be able to be restored to an acceptable moisture level within 48 hours.

Do not freeze paintings, furniture, stone, glass, ceramics, metal, photographs and negatives, or veneered wood objects.

Generally, furniture can be air-dried. Do not rub dirt and mud into the furniture—just rinse and air dry.

There are many professional service firms that can assist in a larger scale flooding clean up, that have access to all the required human resources and equipment. You may be able to handle smaller scale events yourself.

CONCLUSION

In closing, it is important to reinforce a few key ideas:

1) Disaster recovery planning is not magical nor does it require specialized training. It is like the practice of law: it is requires thoughtful analysis and discipline. The discipline cannot be overemphasized. A plan needs to be developed, written down, tested and the users must know if its existence and be trained as to its use.

2) No plan is perfect and all plans are different. No one can anticipate all the elements of a disaster. A plan that is too complicated will likely be ignored at the very time that it needs to be used. Also, it will be too large a task to keep up to date and the cost of developing such a plan will likely result in no plan being developed. Also, every organization is unique and these unique attributes will result in different plans. Start simple and start small. Any plan (even an imperfect one) is better than no plan at all.

3) The purpose of education is not learning, but action. The purpose of disaster recovery is the same—ACTION. It is a call to arms and provides you with the confidence and tools to lead in the most extremely negative circumstances. The execution of your disaster recovery plan will depend on a number of factors but it has been shown, time and time again, that good communication and leadership is what differentiates persons and organizations who successfully survive adverse circumstances from those who do not.

APPENDIX I

POSSIBLE EVENTS AND HAZARD CHECKLIST

The attached list is not a complete list of events or hazards but it is fairly comprehensive. You may find that some are not applicable at all or are very remote. This is a tool to ensure that you have considered a wide spectrum of risks and hazards to ensure a more complete analysis and plan.

Human (including criminal) activity

Theft and robbery
Arson
Bomb and bomb threat
Software failure (e.g. virus, cyber attacks and hacker activity)
Loss of key personnel with essential tasks, keys and codes
Sabotage (disgruntled client, employees, other)
Riot and civil disorder
War and insurrection
Terrorism and hostage events
No access – interruption by civil authority, snowstorm or strike or other disruptions from communications, transportation or service sector
Human error caused by poor training, poor maintenance, carelessness, misconduct, substance abuse or fatigue.

Natural disasters

Snow, blizzard, sleet, hail or ice storm
Tornado, hurricane or windstorm
Forest fire
Severe thunderstorm
Flooding
Prolonged drought
Earthquakes
Mud and landslides
Tidal wave
Volcanic eruption

Infrastructure disasters

Fire or explosion (from an internal or external source)
Smoke damage
Power failure, fuel or energy interruptions
Telecommunications failure
Server or other hardware failure
Flood or water damage (sprinklers)

Water supply failure
Sewer backup or failure
Pollution or chemical spill
Structural collapse
Radiological disaster

Accidents involving

Transportation – motor vehicles, marine, trains and aircraft
Bodily injury
Transportation of chemical or nuclear materials
Broken water and sewer lines
Broken or downed power and communication lines
Broken pipelines

APPENDIX II

EMERGENCY CONTACT LIST

It is very important that you have an emergency contact list at your fingertips. This should include key public and private services and other resources you may need to draw upon. If a certain resource is critical, you may want to include alternate companies or persons in the event they are unable or unavailable to assist.

TIP: *You will be surprised how many times you will use this list. People have found it a useful resource in all sorts of circumstances that would not be classified as disasters.*

Key contact information may include:

- Telephone numbers
- Cell phone numbers
- Fax numbers
- E-mail
- Other contact information (e.g. cottage, boat radio call numbers, etc.)
- Address
- Key contact person
- Materials or service provided (if a supplier)
- File or account numbers, where applicable

Your emergency contact list may include:

- Fire
- Ambulance
- Police
- Friends and neighbours (who may be able to provide personal support)
- Plumber
- Electrician
- Locksmith
- Carpenter
- Power utility
- Gas utility
- Broker/agent (have your insurance company name and policy number)
- Other lawyers (who may be able to provide support)
- Security
- Landlord or building security (if applicable)
- Office supply contact
- Computer supply contact
- IT support personnel
- Local media (radio, TV and newspaper)

- Other contacts (as determined by your disaster recovery plan)

APPENDIX III

COMPUTER INVENTORY

Create a form for your computer hardware, peripherals and software and attach your vendor documentation to this form. Keep a copy of this with your disaster recovery plan. Updating the form after each purchase is a good idea. Vendors include suppliers from which you have purchased, leased or had repairs completed. This is a very useful tool when you are trying to rebuild your office as it will help you easily and quickly determine what you need to buy.

Information to be gathered may include:

- Hardware (e.g. PC, monitors, printers, keyboards, etc.)
- Hardware criteria (e.g. RAM, CPU capacity, size of hard drive, etc.)
- Peripherals such as zip drives, modems, scanners, etc.
- Software (be sure to note title and version and updates and number of licenses and /or license number)
- Model
- Serial Number or ID number
- Date of purchase/lease
- Cost
- Supplier information including company name, address, fax, telephone, e-mail, contact name and account number