

managing
PRACTICE
interruptions





Proficient. Professional. Progressive.

practicePRO is the Lawyers' Professional Indemnity Company's innovative risk management initiative. It is designed to help lawyers adapt to the changing practice climate and to the opportunities that change presents.

Programs. Products. Processes.

practicePRO is a multi-faceted program of tools and resources to help you and your practice thrive.

managing PRACTICE interruptions is just one of several booklets in the practicePRO managing series. Other practicePRO resources available to lawyers include: articles that highlight the profession's legal obligations and liabilities; practice aids that provide a "how to" approach to law practice; information on legal technology; education initiatives; and promotion of the concepts of wellness and balance. For details, please see the back of this booklet.

For more information on how you can put practicePRO to work for your practice see the last page of the book or contact practicePRO at 416-596-4623.

www.practicepro.ca

introduction	3
would you and your practice survive these common disasters?	4
preparing a plan	6
why have a disaster recovery plan?	
how complex should the plan be?	
is your own house in order?	
preparations, processes and procedures	9
establish an emergency response person/team	
establish a damage assessment and reporting person/team	
establish emergency identification and reporting methods	
establish emergency response procedures	
identify and train first aid providers	
create lists of critical contacts	
property and premises: identify, protect and insure	15
inventory	
insurance	
conduct a risk assessment	
space planning	
computer planning and backup best practices	
equipment (non-computer) planning	
preparing your practice for disaster	22
financial continuation	
protecting practice critical documents and files	
protecting client files and documents	
keep your calendar up-to-date	
the emergency buddy option	
how to respond to an emergency	25
the recovery process	26
beginning the recovery process	
complete an after emergency debriefing	
when things return to normal	
reviewing, maintaining and updating your plan	28
establish a safety monitoring person/team	
a marketing opportunity	
summary	29
appendices	30
1 – Other disaster planning and recovery resources	
2 – Other tools and resources from practicePRO	

Copyright Information

Copyright © 2002 by the Lawyers' Professional Indemnity Company (LAWPRO®). All rights reserved. No part of this publication 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, chemical, manual, or otherwise, without the prior written consent of the Lawyers' Professional Indemnity Company, One Dundas Street West, Suite 2200, P.O. Box 75, Toronto, Ontario, Canada, M5G 1Z3.

© Lawyers' Professional Indemnity Company (LAWPRO)

1 Dundas Street West

Suite 2200

P.O. Box 75

Toronto, Ontario, Canada

M5G 1Z3

www.lawpro.ca

LAWPRO and practicePRO are registered trademarks of Lawyers' Professional Indemnity Company.

Disclaimer

This booklet includes techniques which are designed to minimize the likelihood of being sued for professional liability. The material presented does not establish, report, or create the standard of care for lawyers. The material is not a complete analysis of any of the topics covered, and readers should conduct their own appropriate legal research.

The terrible events of September 11, 2001, served to highlight how vulnerable we all are to unexpected accidents or disasters.

Accidents or disasters that have the potential to interrupt or destroy a law practice come in many forms. They can be natural, technology-related, or man-made (both intentional and accidental). They may affect just a single person, everyone at a firm, or even a whole city or region.

Foresight, planning and preparation are critical to minimizing the impact of any accident or disaster, large or small. They may even prevent a minor event from becoming a major one that ends your practice because the stress, panic or emotions of the moment caused you to respond in error or inappropriately.

This booklet provides a comprehensive review of the steps you can take to prepare for unexpected minor and major practice interruptions, and how you should respond to them. It reviews how you can protect your people, your practice, and your premises and property.

Although the suggested preparations and responses may not be relevant to all firms, or to all practice interruptions or disasters, all practitioners will find helpful information in this booklet. Adapt the suggestions to fit your office and resources.

How prepared are you for a serious interruption to your practice? Review the common practice-threats listed on page 4 and consider how your practice would respond.

would you and your practice survive these common disasters?

None of us like to think about disasters, and most of us have an “it won’t happen to me” attitude. This short quiz will help you determine your ability to survive some common “disaster” scenarios.¹

1. If all of the computers in your office were stolen over the weekend, do you have all the serial numbers of the equipment, the original cost of the equipment, the value of the equipment, and the ability to recreate all of the data on the computers?
2. If your office was completely destroyed by fire, how long would it take you to contact all of your clients, recreate all your computer data, contact your insurance company, process invoices, contact opposing counsel and generally get your practice operational again? Who would be responsible for performing each of these functions?
3. If you had a heart attack tonight, are your files organized so that someone could pick up your caseload without your clients suffering any disadvantage?
4. If you could suddenly not come into the office on Monday, have you designated the person who could pick up your caseload? Even if you have a partner, how much does he/she really know about your caseload?
5. If you were unable to come into the office for a few days or weeks, could anyone actually find anything on your desk or in your files? Does the answer change if your assistant was off sick or away on vacation at the same time?
6. If your secretary/legal assistant/bookkeeper suddenly quit, do you know their filing systems so that you can find information in their desks, in their (or your) files, or on their computers? Do you have copies or know where they keep the keys for filing cabinets, etc.? Do you know all their respective passwords (including voice mail, computer login, e-mail, the accounting package and any other software applications they use)?

would you and your practice
survive these common disasters?

7. If one of your staff members disappeared with client trust funds, would you have sufficient records to determine what was taken and when?
8. If you have a partner/associate who was suddenly disabled, do you or someone in your office know his/her schedule for the next three months? Do you or someone in your office know the status of all matters in your office?
9. If you or a partner in your firm were disabled for an extended period of time, will you be able to draw a salary? If so, how much and for how long? If you are a sole practitioner and the only rainmaker, how will expenses of the firm be paid while you are out and unable to make rain?
10. If you were to die or be completely unable to return to work, what would your desk, client files, and office organization say about you to anyone who would have to step in to assume responsibility? What burdens would this place on your partners and spouse? Is this the way you want to be remembered?

If you were unable to answer all of these questions as quickly or as adequately as you would like, then you need to do some disaster recovery planning. Regardless of the size of your firm or practice, you need to create an easy to implement plan which will assist you, or anyone in your office, if there were an unexpected practice interruption affecting you, your staff or your firm.

¹ This was adapted, with permission, from Disaster Planning: Protecting Your Firm, Your Clients And Your Family, 2001, by Patricia Yevics, Director, Law Office Management Maryland State Bar Association, Inc.

Although you're unlikely to ever experience a major, practice-ending disaster, the fact is disaster can strike anyone, anywhere, anytime. More likely you'll have to be prepared to deal with a computer crash or loss of data, theft or malicious damage, fire or flood, or the loss of a key lawyer or staff person. And being prepared involves planning.

Why have a disaster recovery plan?

The better prepared you are to respond to an event that disrupts your practice, the faster you will have your firm back up and running, with minimal financial loss or service interruption. To ensure this continuity – and ability to bounce back quickly – you need a plan. That plan starts with a thorough assessment of your exposure, details how you will minimize the impact of each exposure on your practice, and provides a roadmap for how you will deal with all stages of an emergency or practice interruption.

practicePRO has created a spreadsheet that you can use to help identify and assess your vulnerabilities. It is available for download at www.practicepro.ca/disasterrecovery.

To be successful, the plan needs the support of senior management, and the appropriate allocation of budget and resources. Put your plan in writing, and distribute it to all firm employees (and their family members, if appropriate) to ensure everyone is aware of how to prepare for, and respond to, a practice interruption.

Make two copies of your plan; keep one in the firm disaster recovery file, along with other critical information for responding to a disaster or interruption. Put the second in a secure, offsite location. Some firms post their plans and all supporting information on a secure web site.

How detailed should the plan be?

The larger the firm and the more complex its operations, the more detailed your plan likely will have to be. For example, large firms that have multiple offices often set up mirror servers, with all of the accompanying data and

people issues to manage, while a small firm or sole practitioner might plan to work out of a home office.

As well, the level of detail in your plan will reflect the scope of your recovery planning efforts. Plans typically address two top priorities: the need to ensure the safety of your staff; and the need to recover your data centre and critical applications.

However, many firms today aim to have in place a well-designed and tested practice-wide recovery and continuity plan. This type of plan will address the following:

- **Preparation and Prevention:** Preparation and Prevention are essentially about risk management. What can you do to lessen the possibility or the impact of an adverse interruption or disaster occurring to your practice?
- **Response:** Response is the immediate reaction to an incident or emergency. It addresses matters of personal safety, and the policies, procedures and actions to be followed in the event of a practice interruption.
- **Resumption:** Resumption refers to the process of planning for and/or implementing the resumption of time-sensitive practice operations immediately following a disaster (ideally within a specified time).
- **Recovery:** Recovery is the process of planning for and/or implementing the restoration of all firm operations and services to pre-disaster levels.

A minimal plan

Even if you do not plan to implement a full-scale recovery plan, you can minimize some of your exposures – at relatively little cost – through three very simple steps:

- Make proper backups (see computer planning and backup best practices, page 18)
- Create emergency contact lists (see create lists of critical contacts, page 12)
- Maintain adequate and proper insurance coverage (see insurance, page 15)

Is your own house in order?

Putting your personal house in order could help you and/or your partners deal with a firm emergency. In any emergency, quick access to certain pieces of personal information is essential.

Prepare a list with the following critical personal information (if applicable):

- name, address, passport, health card and social insurance numbers of you and your spouse or partner;
- all of your, and your spouse or partner's, phone numbers (home, work, cell, pager, personal fax, cottage, etc.) and e-mail addresses;
- drivers' license and vehicle insurance information;
- name, phone number and address of one or more emergency contacts;
- other special contact numbers (e.g. daycare for your kids);
- name, address and all phone numbers of your direct employees;
- names, addresses and phone numbers of your personal representative, lawyer, accountant, physician and landlord;
- location of your will, power of attorney and/or trust agreement;
- names, addresses, phone numbers, policy numbers, and contact persons for all insurance policies;
- location, box number, and where to locate key to safe deposit box(es);
- list of contents of safe deposit boxes and signatory information; and
- name, address, phone numbers, account numbers, signatory information on all business financial accounts.

You, and other key partners or employees in your office should have this information at their fingertips, including at your respective homes.

Make a photocopy of everything (both sides) in your wallet, and store this information in one or more safe locations that you or someone else could access. Include the 1-800 numbers for reporting lost credit cards. Having access to this information will save you many hours of work if your wallet is stolen or lost.

Central to any disaster recovery plan are the preparations, processes and procedures that help the firm respond to and recover from a disaster. Equally important will be the person or teams put in place to oversee and direct these tasks. In a small firm, ultimate responsibility may rest with a single person. In a medium or larger firm, the responsibility may be shared by a team.

Establish an emergency response person/team

The emergency response person/team will coordinate preparations for and responses to a disaster. This person or team will provide the required leadership and direction, and will make all final decisions. They will also have to periodically review and update all disaster recovery plans to take into account any changes in personnel or circumstances. (For more details, please see reviewing, maintaining and updating your plan on page 28)

When you establish this central coordinating body, you will have to undertake the following:

- define decision-making authority;
- identify and train members, and name alternatives in case of absence or unavailability;
- communicate to employees details regarding entity function and members; and,
- appoint new members immediately if there is any turnover.

Establish a damage assessment and reporting person/team

Depending on the type of disaster, the firm's office, property and files should be promptly examined to determine the extent of damages, if any. These damage assessment findings should be reported to the emergency response team, who should in turn direct salvage efforts, notify insurance carriers, etc.

This damage assessment should be completed as soon as possible after the disaster occurred. In the case of water damage to paper, deterioration begins within 2-3 hours, and damage due to mould, fungal or bacterial growth can start in just 24 hours. It is incredibly expensive, and often impossible, to salvage water-damaged files and records.

Establish emergency identification and reporting methods

What is a potential emergency or critical incident? You will need to identify the types of potential dangers that should be reported to, or by, firm employees. Designate someone to be responsible for determining when you are in an emergency, how this information is to be communicated to employees, who is to follow-up and how and when to issue the "all clear."

Train employees to recognize and report possible emergencies. This will ensure that any event that has the potential to cause a practice interruption is identified and dealt with as quickly as possible. Provide each employee with phone numbers for police, fire, building security, etc. Also, post emergency phone numbers in prominent locations, such as in your reception area, by all conference rooms and in the kitchen area.

Emergency evacuation procedures

If your building or premises does not have emergency evacuation procedures, develop your own people evacuation plan. Every evacuation plan should address the following:

- Identify escape routes;
- Identify employees who need help during an evacuation, and their location; assign a helper to each, and alternative helpers in case of absence;
- Identify “evacuation marshals” who are responsible for making sure everyone is out of your office, and for securing it when they leave:
 - Assign different people to different areas and entrances;
 - Assign alternates in case the primary person is not present;
 - Make sure people who are assigned this task know where keys are, how to deal with magnetic locks, alarms, and any other necessary information;
- Post a sign on your door indicating the closure, and provide a contact number (ideally have this sign prepared beforehand);
- Include a check-in procedure at a gathering place away from the building to account for everyone;
- Hold regular emergency evacuation drills:
 - Start with announced drills to get the procedure down, and then unannounced drills;
- Establish who is responsible for escorting visitors out;
- Ensure training emphasizes employee responsibility to comply with directions of emergency workers and designated evacuation marshals.

Identify specific items (valuable artwork, key records etc.) to be evacuated from the office in the event of an emergency. This should happen only if time permits, and without endangering people. Assign responsibility for this task, again emphasizing human safety over the rescue of objects.

Identify and train first aid providers

Some health problems and some types of disasters could result in you or your employees requiring medical attention. Prepare for this by taking these steps:

- Have some of your employees complete first aid and CPR training;
- Circulate updated lists of qualified first aid providers (identify these people on your master telephone list);
- Provide a triage/treatment area; and
- Ensure that first aid kits are available, and make sure they are continually stocked.

Create lists of critical contacts

Some emergencies will disrupt normal telephone, e-mail and facsimile communication channels. Without current contact lists, your ability to communicate with staff, clients, and other concerned parties will be limited, if not impossible. Create contact lists for each of these groups. Update these lists regularly. Key partners and employees, as well as emergency team members, should have access to these lists at work and at home.

Employees: A current employee contact list lets you easily contact and account for every employee. Your lists should include:

- full employee name;
- home, cell and other phone numbers;
- home address;
- any special medical information;
- phone number, name and address of spouse or partner's employer;
- emergency contact information, with at least one alternate if possible;
- voicemail password; and
- any computer passwords they use, including the programs for which they are used.

Emergency Contacts: Prepare a list of contacts who could provide emergency-related assistance for follow-up, information, hotlines, access to crisis counselors etc.

Important firm contacts: Create one or more lists of other important firm contacts, and include all necessary contact information. These lists should include:

- **Active clients:** If you don't have access to your office or it was destroyed, this list becomes critical for getting in touch with your clients.
- **Opposing counsel and courts:** This list is important if they need to be contacted concerning pending hearing dates, etc.
- **Landlord, property manager, bank, accountant, payroll company, post office, insurance company and broker:** It may be necessary to contact one of these individuals to deal with disaster-related issues.
- **Suppliers and vendors, etc.:** Contacting the people who provided goods or services to the firm becomes important if you need to replace goods that were destroyed, or require services to support your recovery efforts (for example, installing new software on a replacement computer).

Prepare alternative communications channels

Some emergencies will disrupt normal telephone, e-mail and facsimile communication channels. To prepare for this, consider implementing other communication channels:

- Do you have one or more cell phones that you could use in place of your normal phone?
- Determine availability/procedure to re-route phone lines to an alternative location/person:
 - Identify where the calls should go and who should be there to answer them;
 - Who has the authority and responsibility for implementing this?

- Set-up an emergency communication center and determine how to:
 - Answer normal incoming calls;
 - Respond to employee/client/court/etc. questions;
 - Consider if your employee hotline should allow employees to leave messages.
- Set-up a hotline for employees that would provide them with information (either via a live person or a recorded message).
- Use your Web site, or an alternate Web site, to provide information and updates to all interested parties:
 - So you are not doing it in the middle of a crisis, consider creating the site, or a sub-page for your existing site, before the disaster occurs;
 - Consider if parts of this site should be secure to provide confidential information to employees or clients.
 - Consider if a broadcast e-mail capability would be helpful for communicating with employees, clients or others;
- Are the direct phone lines in your office routed through your phone system server?
 - Sometimes they are not, and if so, may not fail in the event the phone system server does. Can you/should you set this up?

property and premises: identify, protect and insure

Although you may take it for granted, your office, and everything in it, are critical for the operation of your practice. A complete disaster recovery plan includes an up-to-date inventory, proper insurance coverage, taking steps to make your office safer, and in some cases, plans for an alternative office.

Inventory

A detailed inventory of ALL office contents is essential for your disaster recovery plan and insurance purposes. Supplement your inventory with a videotape or photographs of everything in every room of the office. Go into drawers, filing cabinets, storage areas and closets. This is the only way to make sure you have a complete record of everything, including smaller items. Ideally, create a list that includes item description, make, model, serial number, purchase price and date, and supplier. Store a copy of the inventory offsite. Obtain appraisals of any items of significant value. Update your inventory annually or when you purchase anything of significant value.

Insurance

Having adequate insurance in place is one of the best things you can do to prepare for a disaster. Consider all types of insurance, including:

- property insurance (if you own your building);
- contents insurance, including extra riders for computers or other equipment of significant value;
- commercial general liability for third-party bodily injury or property damage;
- business interruption insurance;
- crimes coverage; and
- disability, life, or other appropriate personal coverage.

property and premises:
identify, protect and insure

Review and evaluate the adequacy of your coverage, including any policy limits. Pay particular attention to any stipulations, exclusion clauses, and to what extent consequential losses are covered (they likely are not). Consider if you should get any of the following coverage options:

- replacement value;
- valuable papers coverage, including cost to recreate files;
- loss of income;
- all risks, including flood and earthquake;
- cleaning/restoration costs;
- payment of interim rent;
- sprinkler/water damage; and
- personal items (review if your homeowner's coverage covers these items).

Ensuring you are properly insured is an ongoing process. You should regularly review your circumstances and the adequacy of your coverage, ideally annually. Be conservative in making your estimates, and consult with your broker. Some firms tie a coverage review into the renewal process as a way to ensure this task takes place annually. Review your coverage if you make any significant purchases or if there are any changes of circumstance that warrant coverage changes.

Conduct a risk assessment

Does your office have adequate protection and is it as safe and secure as it could be? Conduct a risk assessment to make sure your office has:

- proper lighting, including emergency lighting;
- a working fire alarm or smoke detector;
- fully charged fire extinguishers;
- a CO (carbon monoxide) detector;
- sprinklers;

property and premises:
identify, protect and insure

- fire-resistant, and where appropriate, fireproof safes;
- proper locks and an alarm system;
- a staff member in your reception area to greet visitors at all times;
- cable locks on laptops;
- bookshelves that are secured with bolts to the wall (to prevent them from tipping); and
- a good stock of emergency supplies (flashlights, a radio, cell phones, batteries, candles, blankets, water, toilet paper, and non-perishable food).

Space planning

A fire or a major natural disaster could completely destroy your office, or prevent you from accessing it. To plan for this eventuality, identify a possible temporary office space or "hot site."

If you are in a major urban centre, or want to take extra precautions, consider looking for space away from your immediate area so that you don't find yourself in a situation where a large disaster prevents you from getting to both your main and alternate offices. Larger law firms may need to set-up an alternative office that can function as a new central hub for main office functions. Small firms and sole practitioners could plan to work out of someone's home, in space at another office, or if need be, any vacant building.

Remember, recreating a destroyed office involves more than the simple restoration of your backup data. Determine how work will be assigned, who will do it and how, and how supervision will occur. Identify what tasks or functions could be performed via telecommuting, and identify employees who are suitable and equipped to telecommute. Many law firms already have their lawyers set up to work remotely from home. Consider whether this is an option, and if so, make sure home computers have all standard office software on them.

Computer planning and backup best practices

Computers and other legal technology have become a critical part of practising law. Every law firm has huge amounts of irreplaceable data on server and/or desktop hard drives. The most critical part of any disaster recovery plan is backing up the data on your firm's computers. A backup will allow you to recover when hard drives are lost or damaged (due to theft or fire), or when they fail. Computer hard drives are complex pieces of electronic hardware which have moving parts. All hard drives are subject to failure, and most ultimately will if they are used long enough.

You should do the following things to ensure you have a complete and reliable backup:

- **Do a full backup:** Full backups are preferred to partial backups. Having everything that was on your hard drive is better than finding out you need a critical file that isn't in your backup and is not otherwise available.
- **Do backups daily:** Modern backup hardware is able to do complete backups of large hard drives in a matter of hours. Backups can be set to run automatically, usually in the middle of the night. Doing a daily backup ensures you are as up-to-date as possible. It will have all of the work and data that you created up until the end of the previous day.
- **Identify responsible person(s) and alternatives:** Doing the backup should be a mandatory responsibility that is assigned to a specific individual, and a specific alternate individual. You want to ensure that a backup is done every day, without fail.
- **Review the backup log:** Most backup software programs create a log report when a backup is completed. This report details what was backed up, and if there were any problems.

property and premises:

identify, protect and insure

- **Regularly do test restores:** Don't believe the backup log. Periodically it will report successfully completing a backup, despite the fact that some or all of the data to be backed up was missed. The only way to truly test your backup is to regularly do a test restore of selected files and folders.
- **Identify offsite storage location:** Tapes left on top of your server in your office will be destroyed or taken along with your server if there is a fire or theft. You should store at least some backup tapes in one or more safe off-site locations.
- **Rotate and keep generations of tapes:** Don't use the same tape over and over; rotate your backup tapes. For example, use a series of five tapes, one for each night of the week. This can be helpful when database corruption is detected sometime after it occurred. Having an older backup will allow you to reach back to an earlier date if necessary. Some firms keep end of week, end of month or end of year backups.
- **Replace tapes regularly:** Backup tapes degrade over time and with use. You should replace your backup tapes every six months. When they get to the end of their life rotate them out as end of month tape etc.
- **Don't forget data on desktops, laptops and PDAs:** Usually server backups are configured to only backup data on servers. Make sure that data on desktop computers, laptops and PDAs (Personal Digital Assistants) gets backed up as well. Also have staff back up the phone numbers stored in their cell phones.

property and premises:
identify, protect and insure

- **Make sure open files are being backed up:** Some backup software, and in particular older versions, will not back up files that are in use or “open” by other programs. Central accounting system, e-mail and other database files often remain open 24 hours a day. Make sure that your backup is getting all open files.
- **Create written instructions for restoring:** Many offices have one or two people who know how to do a backup, but no one who knows how to restore backed up data. Create written instructions and train several people to do this task.
- **Find a hardware backup buddy:** If your backup server and tape unit are destroyed or stolen, you could find yourself with a good backup tape and no compatible tape unit to do a restore. Ideally find someone who has a server and tape unit that is identical to yours.

A partial backup from last week is better than no backup at all. If you aren't doing full regular backups, at least spend some time backing up some of your important files. It is easy to copy files onto a CD or some type of removable storage device. It is even easier to simply copy them to another computer on the network. This won't help if your office burns down, but it will if you have a hard drive failure.

Other computer issues

Protect your investment in your computer systems – and the information stored on them – by doing the following:

- Identify sources of rental/loaner computer equipment, and service people with necessary expertise to support it;
- Use uninterruptible power supplies (UPS) and surge protectors, especially on servers and phone systems;

property and premises:
identify, protect and insure

- Use anti-virus software, and keep virus definition files up to date (at least weekly, this can be set up to happen automatically);
- Implement appropriate security on your servers and networks; and
- Use firewalls at any external network access points.

It is important to document all new programs, updates, patches, modifications and customizations to computer systems, and to store a hard copy of this documentation off site, along with software license numbers, activation codes and copies of original CD's. You should also have documentation that sets out how the standard installation and set-up of all programs on a standard office PC. This will allow you to recreate one from scratch if necessary or create a prototype for a quick restoration.

Equipment (non-computer) planning

As well as computers, you will need many other types of equipment if you need to set up an office at an alternate location. To prepare, consider the following:

- Identify the other types of equipment you may need: including telephone systems, photocopiers, printers, facsimile machines, network hardware etc.;
- Consider taking older, unused equipment to your off-site or home office;
- Identify sources of rental or loaner equipment, and service people with the necessary expertise to support it;
- Store a limited amount of basic office supplies at home or in your off-site location as well.

This section reviews the steps you can take within your practice to prepare it for an unexpected interruption or disaster.

Preparing to meet financial needs

Any disruption to a firm's revenue stream, especially a disruption that lasts for some time, can have a significant impact on a firm. As well as the usual ongoing expenses, such as payroll, you may have to finance a myriad of disaster-related costs. To prepare, include the following measures in your plan:

- **Regularly back up all financial and billing programs:** This will insure that you have access to all critical financial information, including accounts payable, accounts receivable, dockets, client WIP and disbursements, and accounts receivables.
- **Store some blank cheques in a secure, off site location:** A small supply of company cheques helps communicate that it's "business as usual."
- **Arrange a line of credit:** A line of credit can be a lifeline, ensuring cash flow until you can get your billing and collection procedures back in place.

Protecting practice critical documents and files

Having off-site copies of critical, practice-related documents could be helpful if your office is destroyed or can't be accessed. Consider keeping copies of the following documents in a secure, off-site location:

- your disaster recovery file and all supporting information (contact lists etc.);
- partnership and other firm-related agreements and documents (including minute book);
- leases or sub-leases;
- insurance policy and broker information;
- inventory list, including videotape or photographs if taken;
- employee contact list; and
- any other important administrative records or documents.

Protecting client files and documents

Your client files contain irreplaceable information. Reconstructing a lost file is a very time-consuming process. In most cases you will never be able to completely reconstruct everything that was in a lost file.

Take the following steps to protect the contents of your client files:

- **Keep active files up to date and well organized:** This will help you, or your replacement, find file information when resources are limited and stress is high.
- **Properly store files and documents:** Don't leave your files on desks, chairs, the floor, windowsills. Anything left out is more susceptible to theft, fire, water or smoke damage. They should be placed in a fire resistant filing cabinet.
- **Take extra precautions with irreplaceable documents:** Client originals and other irreplaceable documents should be stored in a fire-proof safe (not a fire-resistant one).
- **Don't put critical documents or files on or near the floor:** This can help minimize the potential of water damage.
- **Store photographs and negatives separately:** Keeping them separate may be a life saver in the event one set is damaged or destroyed.

Keep your calendar up-to-date

Almost all areas of law practice are deadline driven to some degree. Areas such as litigation live and die by deadlines. For this reason it is critical for lawyers to keep an up-to-date calendar.

Take the following steps to protect this information and make it available to others in an emergency:

- **Have a current calendar in at least two different places:** This can include at your office and/or at home.
- **Make sure others have access to it:** In addition to your own support staff, one or more other staff or lawyers at your firm should have access to your calendar in case both you and your staff are unavailable.

The emergency buddy option

All lawyers, and in particular sole practitioners, should reflect on the issue of who would step into their shoes in the event of incapacitation or death. In larger and medium-sized firms someone else in the same practice area may be available to take over a disabled lawyer's practice.

However, lawyers in small firms may not have someone with the necessary expertise or capacity to take over. One possible solution is an "emergency buddy" – a qualified peer who can help notify clients, take on your caseload and run your practice in case of personal emergency or other disasters. Consider making this a reciprocal arrangement: You each agree to step into each other's shoes. It may make sense to arrange for your files to go to two or more lawyers.

If your buddy is at another firm, be aware of and follow the applicable ethical requirements regarding conflicts, advance client consent, etc. Regularly provide your buddy with any updated information necessary to carry out his/her role. Make sure your staff are aware of your plans as they may be inclined to send your files to someone else. You can adapt and follow the procedures outlined in this booklet, to the extent applicable, based on your staffing, location, etc.

h o w t o r e s p o n d t o a n e m e r g e n c y

During any emergency human life and safety come first. Evacuate, contact and account for all people in your office. Obtain emergency medical attention for anyone who requires it.

Once you are certain that all of your staff are safe, implement your disaster recovery plan and respond to the specific circumstances of the emergency:

- **Review the disaster recovery file:** In the heat of the moment mistakes can be made and steps can be missed. Review and start to execute the plans in the disaster recovery file.
- **Report to authorities:** Make any necessary reports to the appropriate authorities.
- **Rescue critical records and valuable property:** If time and safety permit, rescue any identified critical records and valuable property.
- **Mobilize your emergency response person/team:** Bring together the people who have been charged with responding to an emergency.
- **Move to the recovery process:** Put the people and resources in place to start the recovery process.
- **Make maximum withdrawal from ATM:** This will give you some cash in case banking or ATM services are unavailable for a short period of time.

Beginning the recovery process

The recovery process starts as soon as the emergency ends. Implement the appropriate steps outlined in your plan for managing disasters and/or business interruptions:

- Access and review your disaster recovery file to determine the appropriate next steps and to ensure you have access to all of the required information.
- Attend to less critical physical and emotional needs of employees:
 - Implement any assistance provided through benefits' plans, counseling services or EAPs (Employee Assistance Plans).
- Mobilize the damage assessment person/team:
 - Initiate immediate actions necessary to protect and preserve property and records, and to eliminate ongoing hazards;
 - Determine salvage and recovery requirements and time frames; notify insurance carriers as they may provide direction and resources for the salvage efforts.
- Contact all employees for after-hour emergencies, and employees who were absent from work for work-hour emergencies, and confirm procedures to provide interim status updates.
- In case of a natural disaster, contact the local emergency operations centre to get directions and status information.
- Implement an Emergency Communications Center: Start re-routing phone lines, identify an alternate Web site etc.
- Review your insurance policies, and contact appropriate brokers and insurers.
- Begin the notification process (clients, courts, opposing counsel, post office, vendors and suppliers, etc.).
- Review calendars to identify tasks that have upcoming deadlines, and assign any tasks that have to be dealt with to an appropriate person.

- Initiate a search for and transition to temporary space if this is necessary; start sourcing other furniture, equipment, and supplies.
- Help set up employees who will be working from home.
- Implement other aspects of the disaster recovery plan as applicable.

For insurance purposes you should carefully document all work done and expenses incurred on disaster recovery-related tasks. Make detailed docketts of all time spent, both billable and non-billable.

Expect the unexpected. There will always be something you didn't plan for or expect. Don't be afraid to ask for help. In a serious emergency, even your opponents may be your lifeline. Offer help to others if possible. They may be worse off than you.

Complete a post-emergency debriefing

After the emergency is over, and when the recovery is well underway, you should hold a debriefing for your staff. Bring everyone together and thank them for their responses, and their understanding of any ongoing inconveniences. Respond to their concerns and provide as much information as possible about the status of the situation, and future plans. A group hug is an important part of the recovery process. Seek input from everyone about what went well, and what didn't. Respond and address any new issues raised, and obtain any additional resources suggested in the debriefing.

When things return to normal

Again assemble your entire staff and thank them for their responses and understanding. Celebrate the creativity and caring that occurred in the face of disaster. This is important for the healing process. It may take some employees a long time to put the disaster behind them.

Revisit your disaster plan, using the experience to improve your plan.

reviewing, maintaining and updating your plan

The ultimate test of any practice continuity plan is that it works when it is needed. Test your plan to ensure it covers everything it should. Determine if the procedures and people you have in place do work. Remember that employees come and go, and computer equipment gets moved and replaced.

Link your review of the plan to another annual event, such as the renewal of insurance coverage. At the same time, review and update your inventory, all contact lists, and the insurance coverage itself.

Establish a safety monitoring person/team

Keeping things safe is an ongoing responsibility. Consider having a safety monitoring person or team whose responsibilities can include:

- regularly looking for hazards (overloaded electrical circuits, improper use of extension cords, blocked stairways and exits etc.);
- verifying exits are clearly marked;
- making sure fire extinguishers are available and charged;
- stocking emergency supplies and making sure first aid kits are complete;
- conducting safety training for employees; and
- organizing new employee orientation.

A marketing opportunity

Some clients will be impressed by a firm that has a solid disaster prevention and recovery program in place. If appropriate, tell your clients about your preparation, emphasizing your disaster preparedness as evidence of your firm's flexibility, strength and reliability.

LAWPRO encourages lawyers and law firms alike to be proactive in preparing and planning for practice interruptions and disasters, not only because we believe it can help reduce claims, but also because it fundamentally strengthens individual lawyers and their practices.

This booklet is but one tool to help you prepare for and manage business interruptions, large or small. It will help you determine where you are most vulnerable, how you can address these vulnerabilities, and minimize the impact an interruption will have on your practice.

If you suffer a minor disruption, your preparations should allow you to recover with only minor inconveniences. If you suffer a major disaster, the time and money invested now could be returned many times over, and may even save your practice.

Appendix 1 lists other resources that can help in disaster prevention and recovery planning.

Other disaster planning and recovery resources

Books

Disaster Survival Planning: A Practical Guide for Businesses,
by Judy Kay Bell; Disaster Survival Planning, 2000

Step-by-step instructions on what you need to do to create, develop, implement, and test your own disaster recovery plans.

Emergency Management for Records & Information Programs,
by Virginia A. Jones and Kris E. Keyes; ARMA International; 2001

A guide through the essential phases of emergency management: prevention, preparedness, response and recovery, with a focus on handling electronic records.

Handbook For The Recovery Of Water Damaged Business Records,
by Julia Niebuhr Eulenberg; Association of Records Managers, 1986

How to recover files that have sustained water damage, with some information on fire and smoke damage, as well as chemical contamination.

Manager's Guide To Contingency Planning For Disasters: Protecting Vital Facilities And Critical Operations 2nd Ed., by Kenneth N. Myers; John Wiley & Sons; 1999

A focus on contingency planning, and provides sample computer contingency plans and business-continuity strategies and case studies.

Managing Emergency Situations in Law Firms: Minimizing the Damage,
by Nina Wendt and L.J. Sklenar; Kendall/Hunt Publishing Company, 1993

Coverage of almost every conceivable disaster for which a firm must prepare, and how to avoid or recover from them, including sample disaster recovery plans

Websites

ABA Crisis Management Resources Bibliography:

www.abanet.org/barserv/disaster/disasterbiblio.html

An extensive list of law firm crisis management resources from the American Bar Association, including books, articles and online resources:

Disaster Recovery Journal: www.drj.com

There is helpful information on the website of this monthly publication, which is dedicated to the field of disaster recovery and business continuity.

INFOSYSSEC: www.infosyssec.org/infosyssec/buscon1.htm

An overwhelming collection of links to business continuity and disaster recovery planning information.

Northeast Document Conservation Center: www.nedcc.org

A nonprofit entity that provides document conservation advice and services. There is information on the site for drying wet documents, and dealing with fire, pests and mould damage.

Office of Critical Infrastructure Protection and Emergency Preparedness:

www.ociepc-bpiepc.gc.ca

This is the Canadian equivalent of the US Federal Emergency Management Agency or FEMA (www.fema.gov).

Red Cross: www.redcross.ca and www.redcross.org

For major disasters the Red Cross can be a helpful source of information and resources.

Other tools and resources from practicePRO

practicePRO provides lawyers with a variety of tools and resources, in both print and electronic formats, designed to help your practice grow and thrive.

The “managing” series of booklets:

These booklets provide insights and checklists to help lawyers better manage the risk associated with specific practice issues. Titles include: *managing the lawyer/client relationship*; *managing conflicts of interest*; *managing the practice of investing in clients*; and *managing a mentoring relationship*.

The Online Coaching Centre (OCC)

The OCC is an online, self-coaching tool, comprising more than 150 modules, to help lawyers become more productive and effective in their professional and personal lives. Topics covered include: communicating powerfully; managing stress; overcoming procrastination; managing practice more efficiently; developing new business opportunities; and capitalizing on emotional intelligence.

Technology resources

practicePRO helps lawyers integrate technology into their practices through: the practicePRO Technology Roadshow; practicePRO Technology Breakfasts; and a bi-weekly practicePRO Technology Tip.

Wellness resources

The practicePRO Web site provides an extensive listing of links to assessment tools, guides and resources to help lawyers address wellness and balance issues.

Special Reports

Special Report on Litigation explores the increase in litigation claims, the forces driving change in litigation practice and the types of errors that underlie litigation claims, and provides practice management tips to help reduce exposure to claims.

Special Report on Fraud examines the new real estate fraud, which increasingly targets lawyers, and provides tips to help lawyers avoid being caught.

For more information visit www.practicepro.ca or call 416-596-4623.

About the Author:

This material was prepared for the Lawyers' Professional Indemnity Company (LAWPRO®) by Daniel E. Pinnington, Director, practicePRO (dan.pinnington@lawpro.ca). Parts of this booklet were adapted, with permission, from a checklist written by Diane M. Ellis, State Bar of Arizona, which was based on materials developed by other Practice Management Advisors.

Lawyers' Professional Indemnity Company
One Dundas Street West
Suite 2200, P.O. Box 75
Toronto, Ontario M5G 1Z3

www.lawpro.ca

