

SURVIVRE AU CHAOS EN PÉRIODE DE CRISE :
Plan en prévision de désastre pour les petits et moyens cabinets juridiques

Par Robert Patzelt

Décembre 2003
L'Association du Barreau canadien

SURVIVRE AU CHAOS EN PÉRIODE DE CRISE

*Plan en prévision de désastre pour les petits et moyens cabinets juridiques
(utile aussi pour les grands cabinets !)*

TABLE DES MATIÈRES

Introduction et avis de non-responsabilité

Rétablissement après désastre

Plan de rétablissement après désastre

Introduction

Objectif du plan

Le plan

Attitudes requises pour la préparation de plans en prévision de catastrophe

Production du plan

Formation et essais : les clés du succès

Fichiers de secours en cas de désastre

Évaluation des risques

Préparation – que faut-il faire faire avant un désastre

Polices d'assurances

Protection physique

Sécurité

Séismes

Préavis

Protection informatique

Faire face au désastre

Indices d'un besoin de counselling ou d'assistance

Aide aux employées, employés

N'oubliez pas les enfants

Rapports avec les assureurs

Protection contre les dégâts d'eau

Conclusion

Annexes :

Liste de contrôle des événements possibles et des risques

Activité humaine (y compris l'activité criminelle)
Désastres naturels
Désastres d'infrastructure
Accidents divers

Liste de ressources d'urgence

Inventaire informatique

SURVIVRE AU CHAOS EN PÉRIODE DE CRISE

*Plan en prévision de désastre pour les petits et moyens cabinets juridiques
(utile aussi pour les grands cabinets !)*

« La vie, c'est ce qui vous arrive pendant que vous faites d'autres projets. » John Lennon

INTRODUCTION

À notre époque, planifier l'impensable est devenu essentiel pour toute entreprise, y compris les cabinets juridiques. En tant qu'avocats et avocates, on nous demande d'aider nos clients et nos clientes dans les moments de détresse et de difficultés, mais serions-nous prêts à faire face à l'adversité si notre cabinet était soumis à un événement ou à une série d'événements qui entravaient sa capacité de poursuivre ses activités normales ?

Cette ressource documentaire est offerte aux membres de l'ABC pour qu'ils puissent être en position de faire face à toute catastrophe – des problèmes informatiques à la destruction complète de leur bureau.

désastre : événement funeste, malheur très grave; dégât, ruine qui en résulte.

rétablissement : action de rétablir; remise en fonction ou en vigueur; retour à la santé.

Le petit Robert, dictionnaire de la langue française, édition mise à jour, Dictionnaires Le Robert, Paris.

AVIS DE NON-RESPONSABILITÉ

Ce document contient des données, des commentaires, des listes de contrôle et des tableaux qui ont pour but de minimiser les dommages et les conséquences négatives résultant de pertes, en particulier celles qui entraînent des interruptions de service. Il ne s'agit pas d'une analyse complète des thèmes couverts, et les lecteurs et lectrices ont tout avantage à entreprendre leur propre recherche et analyse, fonctionnelle, juridique ou autre.

© 2003, Sanddollar Analytics Inc. Tous droits réservés. Cette ressource documentaire a été offerte à l'Association du Barreau canadien (ABC) sous licence, à l'intention des seuls membres de l'ABC, qui peuvent la visionner, la télécharger ou la copier à des fins professionnelles, pour usage dans leur cabinet juridique. Aucune partie de ce document ne peut être transcrite, reproduite ou conservée dans un système accessible ou traduite dans une langue ou un langage informatique sous toute forme ou par tout moyen, mécanique, électronique, magnétique, optique, manuel ou autre sans le consentement écrit préalable de Sanddollar Analytics Inc. Toute demande d'autorisation peut être acheminée par le biais de l'ABC.

RÉTABLISSEMENT APRÈS DÉSASTRE

Ce document a été rédigé en 2003, une année durant laquelle les Canadiens et Canadiennes se sont retrouvés à la merci d'une série de désastres importants, y compris une épidémie de SRAS, une panne majeure de courant, des incendies de forêts destructeurs dans l'Ouest canadien et l'ouragan Juan dans les provinces atlantiques. Tous ces événements sont survenus en moins d'un an et tous servent à rappeler que nous ne pouvons plus compter que le cours des choses suive toujours le scénario des « affaires comme à l'habitude ». Un événement catastrophique peut se produire en tout temps et souvent, sans avertissement.

En 2001, les États-Unis ont été soumis à l'attaque terroriste la plus dévastatrice de l'histoire, et ses effets se font toujours sentir aujourd'hui. L'Association du Barreau de New York estime que des milliers d'avocats et d'avocates ont dû se relocaliser à cause de la destruction du World Trade Center.

À part la terrible tragédie humaine, les événements de cette journée fatidique ont eu pour effet de réorienter les efforts de redressement, qui avaient jusque là porté principalement sur les technologies de l'information, vers les enjeux de continuité des affaires : comment communiquer, comment rester en affaires, comment revenir le plus vite possible aux « affaires comme à l'habitude ». Voici quelques-unes des leçons apprises :

- * Des membres essentiels du personnel peuvent ne pas être disponibles.
- * Les communications – téléphone, Internet et fax – sont essentielles. Voir **LISTE DE RESSOURCES D'URGENCE**.
- * Les plans de rétablissement après désastre sont essentiels; ils doivent en outre être mis à jour, testés et conservés en sûreté, à l'extérieur du bureau.
- * Les vulnérabilités, les forces et les dépendances doivent être correctement analysées.
- * Les employés, employées, sont essentiels, ainsi que les plans de communications et les moyens d'assurer leur mise en oeuvre. Voir **FAIRE FACE AU DÉSASTRE** pour des renseignements additionnels sur l'assistance requise durant les périodes de grand stress.

Plusieurs personnes fonctionnent en croyant qu'une crise, ça n'arrive qu'aux autres. D'autres croient que les caractéristiques uniques de leur organisation les immunisent contre les conséquences négatives d'un désastre. Par exemple, ils peuvent avoir le sentiment que leurs organisations sont trop petites pour subir des conséquences graves. De fait, le contraire peut être vrai. Des organisations plus petites peuvent manquer d'élan ou posséder insuffisamment de redondances pour leur permettre de faire face à d'intenses pressions.

Des désastres comme les attaques terroristes contre le World Trade Center et la panne massive du mois d'août 2003 font inévitablement les manchettes et captent notre attention, mais la majorité des désastres sont des « catastrophes tranquilles », comme une panne d'ordinateur ou la perte d'une ou d'un employé clé. Êtes-vous préparés à affronter de tels imprévus ?

Quelles sont les conséquences d'une panne informatique majeure pour votre cabinet ? On estime qu'environ 45 pour cent de toutes les pertes de données d'ordinateur sont causées par des surtensions électriques ou des pannes de courant. On estime que les systèmes d'ordinateurs et de

télécommunications subissent environ 120 problèmes électriques à tous les mois. Durant un désastre, il y a une augmentation marquée des communications téléphoniques, qui peut s'accompagner d'une perte simultanée des moyens de télécommunications, laquelle peut aussi perturber le fonctionnement normal du cabinet. De plus, les ordinateurs peuvent être menacés autrement, notamment par des pannes de quincaillerie, des erreurs de logiciels, des virus et des pirates informatiques, sans oublier le vol. Voir **RISQUES POUR LES DONNÉES**.

Quand un incendie endommage ou détruit votre bureau, êtes-vous en mesure d'enclencher rapidement et efficacement les démarches auprès de votre assureur ? Êtes-vous en mesure de faire de la facturation et de poursuivre vos activités ? La majorité des incendies ont lieu à l'extérieur des heures normales de bureau (70 pour cent des incendies de bureau se déclarent entre 21 heures et 9 heures) quand il n'y a personne pour sonner l'alarme, pour appeler le service des incendies ou pour éteindre le feu. En se préparant pour les désastres et leurs conséquences, il faut surtout reconnaître que les désastres ont des formes variées et que personne n'y est immunisé. Pour une liste plus complète, voir la **LISTE DE CONTRÔLE DES ÉVÉNEMENTS ET RISQUES**. Cela dit, une approche proactive à la planification antisinistre peut aider à prévenir des incidents négatifs, à minimiser leur impact et à revenir dès que possible et le plus efficacement possible à la normale.

PLAN DE RÉTABLISSEMENT APRÈS DÉSASTRE

INTRODUCTION

Un plan de rétablissement après désastre permet d'assurer que les services et produits essentiels soient disponibles durant et après un incident perturbateur, permettant au cabinet de retrouver ses bureaux, ses données et ses biens plus rapidement. Parmi les principaux jalons du processus, mentionnons l'identification des ressources nécessaires à la poursuite des affaires y compris le personnel, l'équipement, les renseignements, les données et les autres exigences organisationnelles (aussi appelées planification de la continuité des affaires). Tout plan de rétablissement après désastre devrait être un processus proactif qui inclut :

- * les mesures à prendre
- * les ressources à utiliser, et
- * les procédures à suivre.

OBJECTIF DU PLAN

En bref, vous essayez de :

- * réduire les risques de pertes. Un cabinet mettra naturellement l'accent sur les locaux physiques, l'équipement informatique, l'équipement de communications (notamment le téléphone, le télécopieur et l'Internet), les dossiers et documents de clients et clientes, les finances et la comptabilité.
- * proposer des moyens rentables de se préparer aux risques. Cela se raccorde à la couverture d'assurances et, à plus long terme, réduit les frais d'assurances.
- * assurer un rétablissement rapide et ordonné (éviter la panique). La communication est essentielle pour rassurer les employées, employés, et clientes, clients, pour contrôler les rumeurs et gérer les relations avec les médias. Si vous contrôlez la situation et êtes en position de pouvoir exercer un leadership, les clients et les autres seront rassurés et vous appuieront durant la crise.

LE PLAN

Un plan de rétablissement après désastre comprend des solutions de rechange pour la poursuite des affaires et se divise en trois parties chronologiques :

* *réponse à l'incident*

- prendre charge

- communiquer avec les services d'urgence au besoin (service des incendies, ambulances, corps policiers, etc.)
- un plan de notification du personnel et des autres parties intéressées, telles que les clients, assureurs et fournisseurs

- avertir les membres du personnel de leur rôle (où et quand vous aurez besoin d'eux)
- communiquer avec les clients pour passer la situation en revue, discuter des dossiers, etc.
- communiquer avec les fournisseurs
- enclencher le processus de réclamation auprès des assureurs
- rediriger le courrier, les appels téléphoniques, etc.

CONSEIL : *Une communication rapide et efficace constitue l'un des éléments clés d'un rétablissement rapide. Songez à des solutions de rechange, comme des téléphones cellulaires ou des systèmes d'appoint qui redirigent les lignes téléphoniques existantes. N'oubliez pas que durant une panne majeure d'électricité, les communications par télécopieur, par téléphone et par Internet peuvent être gravement entravées.*

CONSEIL : *Intégrez à votre plan une liste de ressources d'urgence – une liste de personnes ressources clés à appeler en cas de désastre. Voir **LISTE DE RESSOURCES D'URGENCE**.*

- identifier les dommages et l'impact potentiel
- mettre le plan en place et coordonner les ressources

** poursuite des services essentiels*

- durant la phase de continuation, la plan aidera à assurer que les services essentiels soient offerts et que leur interruption soit minimisée

- liste de contrôle

- opérations bancaires
- liste de paie
- espace de bureaux et mobilier
- équipement : ordinateur, imprimante, télécopieur, photocopieuse, etc.
- fournitures de bureau : papeterie, cartes d'affaires, etc.

- *rétablissement et redressement*

- réparations et reconstruction
- redéploiement du personnel
- acquisition des ressources nécessaires au rétablissement des opérations normales

ATTITUDES REQUISES POUR LA PRÉPARATION D'UN PLAN EN PRÉVISION DE DÉSASTRE

Préparez-vous au pire, espérez le meilleur. Le pessimisme constitue un élément clé de tout plan en prévision de désastre. Planifiez en fonction de la pire hypothèse. Voici quelques questions à considérer :

Qu'arriverait-il :

- * si vos documents clés étaient détruits dans un incendie ?
- * si l'accès à vos bureaux était interdit pour un temps prolongé ?
- * si un ou plusieurs membres du personnel étaient blessés ou tués ?
- * si vos systèmes informatiques tombaient en panne ?
- * si vos clients et clientes ne pouvaient plus communiquer avec vous ?

L'élaboration du pire scénario est utile. En se préparant au pire, les problèmes mineurs peuvent être réglés plus facilement. Le pire scénario est celui qui empêche le cabinet de poursuivre ses activités, comme un incendie qui détruit vos bureaux.

Quelles fonctions et quels membres du personnel sont essentiels ? Pour bien développer votre plan de rétablissement après désastre, vous devrez passer en revue les tâches de tous les membres du personnel. Qui fait quoi, où et quand ? Analysez vos procédés d'affaires et estimez le temps qu'il faudra, pour certains d'entre eux, de redevenir fonctionnels. Par exemple, l'accès à votre registre d'audiences et à votre calendrier peut être plus critique dans l'immédiat que, disons, les services de paie. Une petite organisation peut simplement émettre des chèques à titre d'avances (des montants proches de ceux qui seraient normalement reçus) et faire les ajustements à une date ultérieure. Obtenir un espace de bureaux peut être plus difficile que remplacer des ordinateurs perdus. Dans un cabinet d'une ou deux personnes, le ou les membres pourraient continuer à travailler à partir de leur domicile, qui pourrait être équipé d'ordinateurs tout à fait compatibles. Par contre, si votre bureau et votre domicile se trouvent au même endroit et qu'ils sont tous deux détruits, votre situation est encore plus pénible. Vous avez le fardeau additionnel d'avoir à régler les questions d'affaires et personnelles en même temps.

Essayez d'identifier les risques auxquels vous pourriez vous trouver confrontés. Plusieurs exemples ont déjà été notés. Demandez-vous ce qui peut arriver à votre personnel, à vos biens matériels et à vos systèmes – juridiques, financiers et techniques. Voyez ce qui peut perturber vos installations, et identifiez les éléments d'information et de communications essentiels, ainsi que les actions avant-pertes en matières d'assurances et de prévention. À la lumière de ces risques, quel est l'impact potentiel et comment vous prépareriez-vous pour garder votre cabinet ouvert ? Pour une liste plus complète, voir **LISTE DE CONTRÔLE DES ÉVÉNEMENTS POSSIBLES ET DES RISQUES**.

CONSEIL : *Chaque plan d'organisation est unique. Concentrez-vous sur les éléments que vous pouvez raisonnablement contrôler et ne vous embourbez pas dans des détails excessifs, surtout quand ils échappent à votre influence. Par exemple, documentez vos systèmes informatiques et leurs éléments pour pouvoir rapidement acquérir un système compatible qui répond à vos besoins. Vous n'avez pas besoin d'une liste complète de tous les fournisseurs potentiels : la compagnie qui vous a vendu votre système actuel constitue un bon point de départ. Gardez les choses simples. Ce document est un guide et une ressource. Personne ne peut prévoir tous les incidents négatifs et se préparer pour toutes les circonstances et conséquences. Il n'est pas nécessaire, non plus, de traiter de chaque catégorie de catastrophe en très grand détail. La perte d'un bureau, que ce soit par incendie ou par inondation, a les mêmes résultats opérationnels. Établissez vos priorités au moyen d'une analyse des risques. Voir **ÉVALUATION DES RISQUES**.*

PRODUCTION DU PLAN DE RÉTABLISSMENT APRÈS DÉSASTRE

Dans le cadre de vos préparatifs de production d'un plan de rétablissement après désastre, vous devriez :

* identifier les procédés essentiels et les échéanciers de rétablissement. Voir **FICHIERS DE SECOURS EN CAS DE DÉSASTRE**.

* établissez des priorités pour les fonctions de votre cabinet juridique. Ces priorités doivent être fondées sur les exigences minimales requises pour réaliser des niveaux acceptables de prestation de services et la période maximale de temps durant laquelle vous pouvez interrompre vos activités sans causer de sérieux dommages à votre situation financière et à votre réputation. Cela inclut une analyse de l'interruption de services pendant des périodes de temps prolongées. La perte de revenus, les dépenses additionnelles et des intangibles comme la perte de réputation comptent parmi les autres impacts à considérer.

CONSEIL : *Si vous ne l'avez pas déjà fait, établissez une marge de crédit qui vous permettra d'avoir accès à des fonds suffisants pour rester à flot jusqu'à la reprise des activités normales. Voir **FICHIERS DE SECOURS EN CAS DE DÉSASTRE** pour d'autres conseils.*

* Définissez vos exigences minimales. Quels éléments sont essentiels au fonctionnement du cabinet ? Que pouvez-vous obtenir temporairement à l'extérieur ?

* Protégez le mieux possible vos exigences minimales, du moins celles qui sont justifiables sur le plan financier. Dans chaque plan, il y aura plusieurs lignes de conduite, mais certaines peuvent être peu réalistes ou économiquement prohibitives. Dans les organisations plus grandes, un réseau redondant pleinement opérationnel peut coûter jusqu'à 3,5 fois plus cher que le système de base. Pour les petites organisations, ce n'est pas pratique, surtout si des éléments clés peuvent fonctionner temporairement sur une base de substitution. Par exemple, un petit cabinet peut avoir la capacité d'exécuter manuellement ce qui est fait électroniquement. Une grande organisation ne peut se permettre un service de paie manuel, mais un petit cabinet le peut. Peut-être le fait-il déjà. De petits cabinets ont peu (ou pas) de personnel en technologies de l'information. Ils n'ont pas de succursales qui peuvent prendre la relève.

* Votre plan doit inclure une documentation écrite pour les réponses, la continuation et le rétablissement.

CONSEIL : *Préparez un plan simple et facile à exécuter. Mettez autant d'information et de détails que possible dans les annexes. La plan devrait se diviser en sections simples et courtes. Utilisez un langage simple et clair. Il s'agit d'un guide pratique – pas d'une prose élégante.*

FORMATION ET ESSAIS : les clés du succès

Testez votre plan et formez les employées, employés. Il est essentiel que les employés connaissent l'existence du plan et son fonctionnement. Ne testez pas le plan lors d'un véritable

désastre : ce n'est pas le temps. Et une simulation de désastre peut coûter très cher et s'avérer très complexe. Il est cependant possible de tester les éléments individuels du plan à différents moments. Un essai partiel permettra de vérifier par exemple si les listes de contacts sont à jour et précises, ou de tester la pyramide d'appels qui permet de joindre tous les membres du cabinet, en conformité avec le plan.

Des exercices sur papier permettent au groupe de prendre connaissance et de tester des éléments du plan. Testez chaque démarche et tentez de déterminer si c'est la démarche indiquée, s'il y a une meilleure façon de l'exécuter et si les actions sont exécutées dans la séquence opportune. Vous pouvez les comparer à votre « pire scénario ». Un peu comme les exercices d'incendie à l'école, vous pouvez créer une fonction similaire dans votre cabinet en testant certains éléments, comme la restauration de données des copies de sauvegarde.

CONSEIL : *L'objectif d'un test est d'éviter les brèches et de faire des améliorations. Si, après avoir complété un test, aucune erreur ou inquiétude n'a été enregistrée, votre examen n'était peut-être pas assez agressif. Un test complet du système pourrait révéler quelques surprises.*

Même avec un plan, il y a beaucoup à faire avant un incident. Deux éléments clés s'adressent aux questions d'assurances. Voir **ASSURANCES AVANT PERTES**. On peut également favoriser la prévention ou la limitation des dégâts. Voir **PROTECTION PHYSIQUE AVANT PERTES**.

CONSEIL : *Rappelez-vous que cette documentation sera peut-être lue et utilisée par d'autres que vous. Assurez-vous d'être clair, pour la personne qui aura à l'exécuter.*

FICHIERS DE SECOURS EN CAS DE DÉSASTRE

Cette activité a pour but d'assurer la protection et la conservation des renseignements essentiels au rétablissement après désastre. Advenant un arrêt complet, les fichiers de données de votre cabinet – listes de clients, de clientes et de renseignements – peuvent avoir plus d'importance et peuvent être plus difficiles à récupérer que les systèmes physiques qui les abritent.

Produisez deux ensembles de fichiers de secours contenant vos données informatiques. Le premier sera conservé dans un coffre à l'épreuve du feu dans votre bureau, et un second à l'extérieur du bureau. Assurez-vous que le site extérieur est suffisamment éloigné pour qu'un incident ou un désastre local ne détruise pas les deux copies de sauvegarde.

Conservez une copie de tous les fournisseurs de services, avec leur nom, leur adresse, leur numéro de téléphone et une personne ressource, pour tous les ordinateurs et équipements essentiels du bureau.

CONSEIL : *Conservez aux mêmes endroits une copie de tous vos numéros de cartes de crédit, de comptes bancaires et de numéros sans frais, comme précaution en cas de vol de votre portefeuille ou de votre bourse.*

Voici une liste de fichiers importants à conserver dans vos fichiers de secours en cas de désastre :

- * les données sur la clientèle : noms, adresses, numéros de dossiers (pour tous les dossiers ouverts). C'est une bonne idée d'avoir un index des dossiers de clients et un index des dossiers conservés à l'extérieur du bureau. Les renseignements sur les conflits d'intérêt sont également très importants.
- * le registre d'audiences et l'agenda des avocates et avocats individuels, ainsi qu'une copie de référence pour le cabinet. N'oubliez pas les renseignements à l'extérieur du système, dans les assistants personnels numériques ou dans les calendriers de poche. Ils pourraient être perdus dans un désastre. **VOIR LISTE DE CONTRÔLE POUR COPIES DE SAUVEGARDE.**
- * les ententes et documents de pratiques et les contrats d'association, y compris les registres de procès-verbaux.
- * les greffiers des différentes cours et les coordonnées du personnel essentiel des principales cours.
- * les noms, adresses, et numéros de téléphone, y compris les cellulaires et les numéros au chalet, de tous les membres du cabinet. Les mots de passe pour la messagerie vocale et les ordinateurs, des renseignements médicaux au besoin. Assurez-vous de conserver ces renseignements et les autres fichiers de secours à des endroits sûrs.
- * les renseignements clés sur les associées, associés, y compris, les NIP, emplacements des testaments, des procurations, des coffrets de sûreté (contenu, information sur les signataires, emplacement de la clef).

- * les numéros d'affaires (p. ex. TPS, TVQ, etc.).
- * les comptes d'affaires et bancaires : noms, adresses, numéros de téléphone, numéros de comptes et information sur le signataires y compris la société responsable du service de paie. Les listes de paie, d'avantages, et autres renseignements sur les ressources humaines peuvent également avoir de l'importance. Les comptes fournisseurs, les comptes clients et autres renseignements financiers essentiels sont tout aussi importants.
- * les noms, adresses, numéros de téléphone, numéros de polices et contacts pour les assureurs, courtiers et agentes, agents, pour toutes les polices d'assurances : biens, erreurs et omissions, responsabilité civile, documents importants, santé, invalidité et vie.
- * contacts d'urgence (représentante ou représentant personnel, médecin, comptable et autres) pour tous les avocats, avocates et membres du personnel, y compris les proches à appeler, les renseignements sur l'école et les soins aux enfants. Pour les avocats pratiquant seuls, il est important d'avoir des avocats suppléants qui peuvent prendre les dossiers en main advenant une blessure ou une maladie.
- * les numéros d'enregistrement et de licence de tous les logiciels du cabinet, y compris les logiciels chargés au préalable sur les ordinateurs.
- * les numéros de série ou d'enregistrement du matériel de bureau (télécopieur, scanners, téléphones, machines à dicter, etc.) et de la quincaillerie informatique; les noms, adresses et numéros de téléphone des fournisseurs et locateurs; les numéros de comptes et de baux (y compris les dates d'expiration).
- * une liste de tous les contrats d'entretien et les renseignements sur les garanties.
- * une liste de tous les achats importants comprenant la date et le prix d'achat (un simple fichier électronique ou un fichier avec reçus et factures).
- * une liste des documents de la bibliothèque et des abonnements.
- * des fonds de caisse et des chèques en blanc. La poursuite des envois de chèques par le cabinet signale que les affaires se poursuivent normalement. Considérez aussi un retrait maximum de votre guichet automatique ou de votre compte bancaire, pour assurer une liquidité advenant une interruption des services bancaires durant cette période critique.
- * songez à conserver du papier en-tête, des enveloppes, et des cartes d'affaires à l'extérieur du bureau. Comme pour les appels redirigés et le paiement des factures avec une réserve de chèques, l'emploi ininterrompu du papier en-tête laisse entendre que tout est sous contrôle.

Les gens ont tendance à mettre l'accent sur les fichiers et dossiers électroniques et souvent, c'est pleinement justifié. Mais il est tout de même important de ne pas trop limiter son champ de vision. Les dossiers englobent bien plus que des fichiers électroniques ou des dossiers écrits. Ils

incluent les journaux personnels, des cartes, des plans, des photos, etc. Même en passant à des systèmes informatiques modernes, certains cabinets conservent toujours des dossiers archivés dans des classeurs, dont nous avons besoin de temps à autre.

ÉVALUATION DES RISQUES

Dans le cadre du processus de rétablissement après désastre, il est utile de préparer un tableau des risques et conséquences. C'est un élément essentiel de l'identification des vulnérabilités. Rien de très élaboré ou complexe : de fait, plus simple est le tableau, plus il sera utile. Voyez ci-dessous quelques exemples. Après avoir énuméré les risques, ainsi que leurs probabilités et conséquences, on peut se concentrer sur les mesures préventives et sur le plan de rétablissement comme tel.

Voici un exemple d'un tableau d'évaluation de risques, avec quelques exemples.

Indice de probabilité :

- 5 - très élevée
- 4 - élevée
- 3 - moyenne
- 2 - contrôlable
- 1 - très faible

Indice d'impact :

- 5 - terminal
- 4 - dévastateur
- 3 - critique
- 2 - contrôlable
- 1 - irritant

Risque (incident ou conséquence)

Associé mort ou gravement blessé

Probabilité (élevée à faible) (5 à 1)

2

Impact humain (élevée à faible) (5 à 1)

5

Impact sur les biens (élevée à faible) (5 à 1)

N/D

Impact sur la pratique (élevée à faible) (5 à 1)

4

Ressources internes

Cabinet de deux associées, associés, seulement; elle est responsable de la plupart des dossiers clients et des conseils spécialisés en fiscalité.

Ressources externes

Nous pouvons obtenir des conseils en fiscalité d'autres cabinets.

Mesures de prévention

S'assurer que les clients et clients sont confortables avec les deux associés, associées, pour minimiser les pertes; établir des contacts dans d'autres champs du droit.

Vol d'ordinateurs au bureau

2 (4 pour les portables)

1

4

4

Autres ordinateurs du cabinet et un vieil ordinateur à la maison; ne suis pas certain si tous les associées, associés, ont les mêmes données.

Possibilité d'achat rapide d'un nouvel ordinateur.

S'assurer que tous les ordinateurs du cabinet sont compatibles; sauvegarde régulière et complète du système d'exploitation, des logiciels et des fichiers; inclure les coordonnées du fournisseur.

Incendie

1 - édifice moderne, bien protégé

4

5

5

Bureaux à domicile

Grande disponibilité d'espace locatif; possibilité d'acquérir du matériel et des fournitures de bureau

Besoin d'assurances suffisantes; d'un système de sauvegarde; assurer compatibilité des bureaux à domicile.

CONSEIL : *Il serait utile de procéder à un remue-méninge avant de faire l'évaluation des risques. Il n'existe pas de bonnes ou de mauvaises réponses. Développez différents scénarios et discutez en groupe des différents éléments. Les différents points de vue seront très instructifs. De plus, toutes sortes d'idées de prévention seront sans doute mises de l'avant.*

PLANIFICATION AVANT-PERTES QUE FAUT-IL FAIRE AVANT UN DÉSASTRE ?

Avec un peu de planification et un peu de chance, il est possible de limiter les dégâts et même d'éviter carrément un désastre.

POLICE D'ASSURANCES

Examinez votre police d'assurances tous les ans. Plusieurs titulaires ont découvert après un sinistre que leur police ne couvrait pas adéquatement leurs véritables pertes. Une assurance insuffisante pourrait être dévastatrice, sur le plan financier.

Passez en revue la liste ci-dessous et discutez-en avec votre conseiller ou votre conseillère en assurances, pour vous assurer que vos besoins sont pleinement satisfaits :

- * Déterminez quels risques ou causes de perte sont couverts par votre police d'assurance. Considérez aussi des questions comme la valeur de remplacement au lieu de la valeur actuelle, une couverture tous risques comprenant les dégâts causés par les inondations, les séismes, les gicleurs et autres dégâts d'eau, les coûts de nettoyage et de restauration, et le paiement d'un loyer temporaire. Ils se peut qu'un avenant à la police ou un endossement spécial soit nécessaire pour ajouter ces couvertures.
- * Considérez la valeur de vos biens en cas de perte.
- * Considérez les niveaux acceptables de franchise, et leur impact sur les primes d'assurances.
- * Déterminez la quantité d'assurances (la valeur à assurer) requise pour éviter des effets surprises de clauses d'assurance partielle.
- * Considérez un endossement pour couvrir les coûts de mises à niveau pour vous conformer aux codes existants.
- * Assurez-vous d'avoir une couverture d'assurances pour d'autres éventualités, telles :
 - une interruption des activités du cabinet (valeur, durée) pour compenser la perte de revenus (si vous êtes propriétaire de l'édifice, il y a possibilité de perte de revenus locatifs)
 - le paiement temporaire d'un loyer
 - des dépenses additionnelles pour couvrir des coûts extraordinaires (location temporaire d'équipement, restauration de données perdues, employées et employés temporaires additionnels)
 - le nettoyage, la restauration, la démolition ou le transport de débris
 - une couverture contre le crime
 - des pannes d'équipement
 - des ordinateurs /les médias électroniques
 - des documents importants, y compris le coût de recréer des fichiers
 - l'assurance invalidité, santé et vie

- * Considérez ce que votre assureur attendra de vous en cas de perte.
- * Considérez le genre de dossiers et de documentation dont vous aurez besoin pour enclencher rapidement et correctement vos démarches d'assurances.
- * Si vous avez un bureau à domicile, songez à inclure les ordinateurs et autres articles de bureau dans votre police d'assurance de propriétaire occupant. Considérez aussi la valeur des articles personnels laissés au bureau du cabinet.
- * Étudiez la possibilité de confier vos assurances maison, biens et automobile au même assureur, pour éviter des brèches dans votre couverture. Notez que les assurances biens ne couvrent pas tous les risques, tels les dégâts d'eau, de neige ou de glace, s'ils sont causés par la négligence du propriétaire ou par une explosion de vapeur (certaines maisons sont chauffées à l'eau chaude).
- * Étudiez la possibilité d'une assurance parapluie de responsabilité civile, pour une somme nominale, afin d'augmenter votre protection contre les sinistres par propagation.

PROTECTION PHYSIQUE

Incendies

Les détecteurs de fumée et de chaleur sont de bons appareils de gestion des risques. Les détecteurs de chaleur sont préférés, étant donné qu'un incendie entraîne une hausse appréciable de la température avant de produire de la fumée. En utilisant un détecteur de fumée, utilisez un bon détecteur à ionisation, qui aura détecté des éléments invisibles dans l'air avant que la fumée ne devienne visible. Rappelez-vous aussi de vérifier les piles fréquemment.

Assurez-vous d'avoir des extincteurs en bon état de fonctionnement, avec une inspection mensuelle et un service annuel. Il est utile, par ailleurs, que tous les membres du personnel soient formés, pour savoir comment s'en servir.

Entreposez les produits inflammables, tels les solvants de nettoyage et autres combustibles, dans des cabinets pare-feu.

Interdisez de fumer, sauf dans une aire fumeurs ou à un endroit désigné à l'extérieur.

Inondations et dégâts d'eau

Pour vous protéger des dégâts d'eau, essayez d'empêcher l'infiltration ou les fuites d'eau, et assurez-vous que vos biens sont situés aussi loin que possible des sources possibles de dégâts d'eau.

Assurez-vous de bien entretenir le toit et de vérifier tout indice d'infiltration d'eau. Les toits plats sont plus vulnérables parce que l'eau s'y accumule davantage, augmentant les chances d'infiltration.

Évitez les entreposages souterrains ou dans des endroits à proximité de tuyaux d'eau et d'égouts.

Faites régulièrement vérifier et entretenir votre système de gicleurs.

Voir **PROTECTION CONTRE LES DÉGÂTS D'EAU**.

SÉCURITÉ

Identifiez clairement les aires fermées au public ou réservées au personnel. Les visiteurs et visiteuses devraient être accompagnés dans ces aires.

Assurez-vous qu'il y ait, dans les aires de réception, un membre du personnel ou un obstacle à l'entrée dans les aires réservées au personnel.

La sécurité physique inclut :

- * sécuriser à intervalles opportuns et à la fin de chaque journée les portes, fenêtres, aires de chargement / réception et autres points d'entrée. Il ne faut pas fermer à clef ou obstruer les sorties d'urgence ou d'incendie.
- * entretenir sur une base régulière les systèmes de contrôle d'accès et les systèmes d'alarme, et former le personnel et les contractuels externes (p. ex. concierge, etc.) à bien s'en servir.
- * s'assurer que les employées, employés, ont un endroit où mettre sous clef leurs objets de valeur (p. ex. bourses, ordinateurs portables, etc.).
- * s'assurer que les employés qui travaillent à une heure tardive peuvent se rendre à leur voiture ou au transport en commun en toute sécurité.
- * s'assurer que les anciens employés rapportent toutes les clefs, cartes d'identité, cartes d'accès, et faire les changements nécessaires aux serrures et codes d'accès.

SÉISMES

Au Canada, les principales zones sismiques sont situées sur la côte ouest et dans la vallée du Saint-Laurent, mais un séisme peut se produire partout. Voici des actions qui peuvent avoir pour effet de minimiser les dommages résultant d'un tremblement de terre :

- * ancrer au mur les bibliothèques et classeurs
- * fixer au mur les chauffe-eau
- * étayer les étagères, les tablettes et autres pour les empêcher de basculer
- * fixer les ordinateurs et petits appareils au bureau avec du Velcro ou un produit similaire
- * verrouiller les tiroirs et meubles pour les empêcher de s'ouvrir

- * utiliser des vis à oeillets fermés pour fixer des articles, tels des tableaux ou des miroirs, aux murs
- * s'assurer que le personnel sache comment trouver et fermer l'eau ou le gaz et installer, avec autorisation, un dispositif de fermeture du gaz.

PRÉAVIS

Dans certaines situations, si vous êtes chanceux, vous aurez un préavis d'un désastre tel qu'une inondation, un ouragan ou une interruption ordonnée par l'autorité civile. Dans ces cas, vous avez l'occasion de vous protéger. Bien sûr une évacuation en toute sécurité constitue une priorité première. Consultez votre plan de rétablissement après désastre, écoutez les bulletins de nouvelles, et prenez les actions préventives suivantes :

- * Sauvegardez vos fichiers d'ordinateur et emportez autant de données informatiques et d'équipement que possible.
- * Fermez tous les interrupteurs principaux et les entrées de gaz. Assurez-vous que vous et votre personnel savez où se trouve votre disjoncteur et qu'il est bien étiqueté. Les locataires peuvent ou non avoir la capacité de fermer leur alimentation électrique, qui peut faire partie d'un système plus grand.
- * Placez les objets de valeur dans un endroit sécuritaire, préférentiellement ailleurs qu'à votre bureau, ou à l'intérieur de l'édifice.
- * Couvrez les biens importants inamovibles avec un plastique épais, et attachez le plastique le plus fermement possible.
- * Fixez les objets sans attache et éloignez-les des portes, des fenêtres ou des aires vitrées.
- * Fermez toutes les portes et fixez les fenêtres pour réduire le danger d'éclats de verre ou de dommages causés par les précipitations ou le vent.
- * Laissez le moins possible d'objets sur le plancher.

CONSEIL : *On ne peut trop insister sur la prévention. Un peu de planification peut minimiser de façon appréciable les effets d'un désastre. Au pire, vous aurez le sentiment d'avoir agi le mieux possible. Dans le meilleur scénario, vous éviterez peut-être une catastrophe ou minimiserez grandement les effets négatifs d'un désastre.*

PROTECTION INFORMATIQUE

CONSEILS DE SÉCURITÉ INFORMATIQUE

On ne peut insister trop sur l'importance de sauvegarder des logiciels et des fichiers de données. Faites des sauvegardes à intervalles réguliers et vérifiez les copies sauvegardées pour vous assurer que les données sont récupérables. Remplacez les bandes de sauvegarde annuellement (préférentiellement à tous les six mois). Il existe sur le marché tout un éventail de bandes de sauvegarde économiques et de dispositifs de stockage amovibles. Assurez-vous de tester votre copie de sauvegarde. Voir **LISTE DE CONTRÔLE POUR COPIES DE SAUVEGARDE**. Vous devez apprendre à vous méfier de l'intégrité de votre système. Rappelez-vous que tous les systèmes informatiques sont sujets aux pannes.

Un des problèmes des systèmes de sauvegarde, c'est qu'ils deviennent désuets aussi rapidement que les autres produits informatiques. Les vieux systèmes de sauvegarde ne permettent souvent pas de sauvegarder des fichiers ouverts. Ces fichiers doivent être considérés, étant donné que plusieurs programmes de courriels et de programmes ou bases de données de gestion sont toujours ouverts. Certaines entreprises se spécialisent dans la récupération de données de bandes et d'équipements désuets ou de disques durs endommagés. Envisagez d'avoir un ordinateur ou un serveur en double avec des logiciels identiques et des capacités de sauvegarde, conservés ailleurs qu'au bureau. Ce peut être une solution pratique pour les avocats, avocates et notaires qui travaillent à la fois au bureau et à domicile.

CONSEIL : *Faites des copies de vos logiciels les plus importants sur des CD. Conservez-les ailleurs qu'au bureau, avec leurs numéros de série, de licence et d'enregistrement. Vous aurez besoin d'un graveur de CD : ces appareils deviennent plus abordables et de plus en plus standards sur les nouveaux ordinateurs.*

Considérez des logiciels d'« écriture miroir » (opération d'écriture s'effectuant simultanément sur l'unité de disque en service et sur un disque miroir, en l'occurrence le disque dur) : si vous subissez une panne de serveur, vous pourrez accéder aux documents sauvegardés depuis 90 jours.

Considérez aussi les technologies de synchronisation des données ou de duplication. Plusieurs logiciels de gestion de causes permettent d'accéder aux registres d'audiences et à l'information sur les causes quand un ou un avocat est sur la route, mais ils effectuent aussi une synchronisation quotidienne pour s'assurer que plusieurs ordinateurs aient la même information. Ainsi, s'il y a une panne de réseau, plus d'un ordinateur a accès aux données essentielles. Une fois que le serveur est réparé et fonctionnel, vous n'avez qu'à resynchroniser, un peu comme si vous synchronisez votre ANP avec votre PC.

La protection contre les virus est un outil essentiel de gestion des risques. Achetez un anti-virus et abonnez-vous à un service de mise à jour en ligne. De nouveaux virus sont créés sans arrêt et vous devez vous assurer que votre protection est constamment mise à jour.

Les utilisateurs et utilisatrices d'Internet devraient utiliser un coupe-feu qu'ils devront régulièrement mettre à l'essai et réparer. Les coupe-feu ont aussi l'avantage de réduire le nombre de fenêtres-pubs irritantes à votre écran.

Développez et mettez en pratique une politique de conservation des dossiers, ainsi qu'un processus de suppression des fichiers. Un tel processus contribuera à vous débarrasser des vieux courriels embarrassants.

Protégez les mots de passe du système en les changeant de façon régulière – des cibles en mouvement sont bien plus difficiles à abattre. Ne donnez pas de mots de passe d'accès à distance à d'autres personnes, même à l'intérieur du cabinet, et n'adoptez pas de mots de passe faciles à deviner (par exemple, votre nom, ou le nom de l'entreprise). Surtout, n'affichez pas les mots de passe à un endroit où ils peuvent être trouvés facilement. Certaines personnes conservent leurs mots de passe dans leur porte-monnaie ou dans leur bourse, sur leur bureau ou affichés sur le mur. Croyez-le ou non, la plupart des pirates informatiques n'utilisent pas la haute technologie pour obtenir leurs accès. Ils utilisent le téléphone, ou fouillent dans les poubelles. Avec l'usage de plus en plus répandu de l'accès à distance, l'intégrité du mot de passe devient encore plus importante. Considérez le cryptage comme moyen de protection accrue.

Développez des politiques et des procédures de sécurité et vérifiez régulièrement qu'on s'y conforme. Si vous êtes une ou un praticien solo ou dans un très petit cabinet, imposez-vous la même discipline que dans un grand cabinet, en changeant fréquemment les mots de passe, etc. Vous êtes tout aussi exposés et peut-être même plus vulnérables.

LISTE DE CONTRÔLE POUR SAUVEGARDES

Le processus humain :

1. À qui a-t-on confié la tâche d'exécuter les sauvegardes ? Assurez-vous qu'elle est confiée à un individu spécifique, y compris à un suppléant ou une suppléante (pour les moments où le premier se trouve en vacances, en congé de maladie, etc.).

2. Créez un ensemble de protocoles. Assurez-vous d'avoir des politiques écrites sur la manière d'exécuter des sauvegardes (voir le processus ci-dessous). L'idéal, c'est d'exécuter des sauvegardes tous les jours, à la même heure, pour développer des automatismes. Certains programmes permettent de réaliser des sauvegardes après les heures normales de bureau. Dépendant de l'ampleur de la sauvegarde, le processus peut durer quelques minutes ou quelques heures. Une sauvegarde a pour but de permettre la restauration de données courantes. Assurez-vous d'avoir des politiques écrites sur la manière de restaurer les données et de former des personnes à cette fin.

CONSEIL : *Vous ne rédigez pas un document sur la sauvegarde du système pour vous-même, mais pour un individu qui ne connaît peut-être pas votre système informatique.*

3. Votre politique doit assurer l'existence d'un registre écrit de toutes les sauvegardes. La plupart des programmes de sauvegarde créent automatiquement un rapport de registres. Examinez le registre périodiquement pour vous assurer que la sauvegarde a été complétée et qu'il n'y a pas eu de problèmes.

4. Testez votre système et votre copie de sauvegarde. Il n'y a qu'une façon de vérifier l'intégrité de votre sauvegarde – c'est de faire une restauration complète. Cela permet de vérifier que la sauvegarde est complète, que l'équipement est compatible et que le processus lui-même est sain. Tenez un registre des qualités de votre système, pour pouvoir en trouver un semblable. Rappelez-vous, votre système informatique peut être endommagé ou détruit et vous aurez besoin de restaurer les données sur un équipement différent.

5. Testez vos systèmes de sauvegarde sur un système informatique compatible pour confirmer davantage l'intégrité du processus. Voici quelques pistes pour assurer une sauvegarde réussie :

* Y a-t-il une configuration et suffisamment de mémoire disponible pour contenir votre base de données de sauvegarde ? Les réglages du serveur peuvent devoir être identiques pour compléter une sauvegarde réussie.

* Les noms d'utilisateurs, d'utilisatrices, et les mots de passe sur votre serveur sont-ils synchronisés avec ceux du serveur sur lequel vous exécutez les restaurations ? Souvent, il y a deux dossiers pour un utilisateur – un au niveau du serveur, l'autre au niveau de la base de données.

* Quelles sont les exigences pour rediriger vos utilisateurs vers un serveur différent ?

Le processus physique :

6. Exécutez des sauvegardes tous les jours. Une sauvegarde quotidienne complète vous assure de données aussi complètes que possible et qu'au pire, votre cabinet ne perd qu'une journée de travail.

7. Assurez-vous d'exécuter une sauvegarde **COMPLÈTE**. Cela inclut les logiciels et les données.

* Sauvegardez tout, ne vous limitez pas à ce qui se trouve sur le serveur. Il faut inclure les données des portables, des ordinateurs personnels (y compris les ordinateurs à domicile) et d'autres équipements tels que les ANP.

* Assurez-vous que les fichiers ouverts sont sauvegardés. Plusieurs courriels, fichiers de bases de données et systèmes comptables sont toujours ouverts. Des fichiers en usage peuvent aussi être ouverts et impossibles à sauvegarder. Des logiciels de sauvegarde plus anciens peuvent ne pas sauvegarder les fichiers ouverts.

Les équipements physiques :

8. Utilisez vos bandes en alternance, et n'utilisez pas la même bande à répétition. Utilisez une série de bandes et prenez la plus vieille bande pour la plus récente sauvegarde. L'avantage des sauvegardes régulières et quotidiennes, c'est que si vous souffrez d'une forme de corruption des données, vous pouvez reculer dans le temps jusqu'au moment précédant la corruption.

CONSEIL : *Apportez seulement la bande sur laquelle vous vous apprêtez à exécuter la copie de sauvegarde. Toutes les autres doivent demeurer dans leur lieu d'entreposage, à l'extérieur du bureau. Vous ne voulez pas regrouper toutes vos bandes de sauvegarde à l'endroit où les sauvegardes sont exécutées.*

9. Remplacez les bandes régulièrement. Le temps et l'usure sont les ennemis de toute pièce d'équipement et les bandes de sauvegarde ne font pas exception. Généralement, les bandes doivent être remplacées à tous les six mois. Vous pouvez utiliser ces bandes pour des sauvegardes plus vastes, comme une fin de mois ou une fin d'année. Envisagez de changer de bandes au moment de passer à l'heure avancée ou de revenir à l'heure normale. C'est un bon aide-mémoire.

Et finalement, le plus important (à part la sauvegarde elle-même) :

10. Assurez-vous d'avoir un lieu d'entreposage à l'extérieur du bureau pour vos bandes de sauvegarde et vos politiques écrites. Vous avez tout avantage à exécuter des sauvegardes entre les ordinateurs et serveurs dans le même bureau, mais cela ne vous servira à rien si la bande repose sur un meuble détruit par le même sinistre qui a dévasté le reste du bureau. Et vous avez besoin non seulement des données mais aussi des procédures de restauration des fichiers.

RISQUES POUR LES DONNÉES

Les ordinateurs sont omniprésents dans l'exercice contemporain du droit. Leur importance ne les immunise cependant pas aux menaces externes, comme les virus ou les dommages physiques, et internes, comme les pannes de système. Une panne de disque dur, par exemple, est l'une des préoccupations les plus communes et déconcertantes pour les utilisateurs et utilisatrices d'ordinateurs. Parmi les autres risques, mentionnons :

* **les pannes de logiciels.** Des designs défectueux ou des bogues informatiques peuvent entraîner la perte de données. Par exemple, en sauvegardant un fichier certains logiciels peuvent supprimer un vieux fichier avant de compléter la sauvegarde du nouveau, au lieu de créer un fichier temporaire et de renommer avec le bon nom de fichier après la sauvegarde. Si, avec ce logiciel fautif, votre ordinateur plante en sauvegardant le fichier, vous pouvez perdre l'ancien et le nouveau.

* **les virus.** Les virus sont des programmes malicieux qui peuvent causer toutes sortes de dommages, y compris la perte de données et même des dommages aux programmes qui tentent d'éliminer le virus. Voir **VIRUS**.

* **l'erreur humaine** . La suppression accidentelle d'un ou de plusieurs fichiers demeure l'une des erreurs les plus communes des utilisateurs. Différents mécanismes – fenêtres de rappel, fonction d'annulation de suppression – existent pour prévenir de tels incidents. Malgré tout, vous pouvez toujours commettre une erreur en sauvegardant sur un fichier existant, ou perdre un fichier en le renommant. Un conseil : changez légèrement le nom des ébauches subséquentes – par exemple liste-dr1.doc, liste.dr2.doc, etc. Votre sauvegarde quotidienne peut aussi vous permettre de réparer une erreur semblable.

* **corruption du système de fichiers** . Il y a plusieurs façons d'endommager ou de corrompre le système de fichiers, sur le disque dur, contenant les programmes et les données. Un bon entretien et un balayage régulier du système de fichiers constituent de bonnes mesures préventives.

* **panne de quincaillerie** . Votre disque dur abrite la plupart de vos programmes et données. Par conséquent, une panne peut devenir un événement très débilitant. Ce risque justifie les sauvegardes quotidiennes. Des pannes de courant au mauvais moment (par exemple au moment d'exécuter des opérations délicates sur le disque dur) peuvent entraîner la perte de nombreux fichiers. Il existe d'autres causes de pertes de données, comme les erreurs de mémoire, etc. Vous n'avez pas besoin d'être une ou un spécialiste de l'informatique pour comprendre l'impact de ces pertes. Il suffit de reconnaître que vos programmes sont à risque et de mettre en place les meilleures mesures de prévention.

CONSEIL : *Achetez des barres de surtension pour tous vos équipements informatiques et téléphoniques. Un éliminateur de surtension avec une batterie de secours aidera à garder vos appareils fonctionnels durant des pannes de courant, le temps de compléter tout au moins un arrêt normal ou une sauvegarde. Une surtension téléphonique peut détruire un ordinateur par la connexion du modem.*

* **malveillance humaine** . Le vol et le sabotage existent, malheureusement. Votre bureau peut subir une effraction ou votre portable peut être subtilisé à l'aéroport. Une ou un employé mécontent peut causer de réels dommages. Les sauvegardes n'empêcheront pas le vol ou le sabotage mais ouvrent la voie à une restauration adéquate.

LES VIRUS

Qu'est-ce qu'un virus ?

Un virus est un programme malicieux conçu, dans sa forme la plus inoffensive, comme nuisance; dans sa forme la plus invasive, il peut causer des dommages irréparables. Les virus peuvent se cacher dans tout programme, sur un CD, sur une disquette, dans des attachements de courriel ou dans des téléchargements de l'Internet.

Une fois qu'un virus s'infiltré dans votre système, il peut se copier sur d'autres fichiers et disques accessibles à l'utilisateur ou l'utilisatrice. Il y a trois grandes catégories de virus : les virus de macro, les virus parasites, et les virus système.

Les virus de macro exécutent automatiquement des commandes de programmes. Ils se reproduisent tout seuls. Si vous accédez à un document qui contient un virus macro et que la macrocommande est exécutée, l'ordinateur devient infecté et tout document sur votre ordinateur qui utilise cette application devient infecté. C'est le type le plus commun de virus et la raison principale de sa propagation, c'est le nombre d'échanges entre utilisateurs et utilisatrices.

Les virus parasites s'attachent à des programmes exécutables et quand vous lancez le programme, vous lancez aussi le virus. Votre système d'exploitation croit erronément que le virus fait partie du programme et lui permet d'accéder à une partie du programme où il peut se reproduire, s'installer dans la mémoire ou libérer sa charge.

Les virus systèmes se greffent sur une zone ou un fichier du système d'exploitation pendant l'opération de démarrage d'un ordinateur. Le logiciel de démarrage est le premier logiciel installé dans votre ordinateur et le virus le remplace avec son propre contenu « modifié ».

Protection antivirus

Voici quelques mesures de protection à votre disposition :

* exécutez des sauvegardes de tous les logiciels, systèmes d'exploitation et fichiers. Si un virus vous infecte, vous pourrez alors restaurer votre système.

* utilisez des logiciels antivirus et mettez-les à jour régulièrement. Cela permet à votre système de détecter, de rapporter et même, dans certains cas, de détruire des virus.

* soyez prudent quant à l'origine de vos programmes, données, etc. Tel qu'indiqué, la capacité d'infection augmente beaucoup quand les utilisateurs et utilisatrices partagent des fichiers. Vérifiez la source de toute information :

- téléchargez avec soin du Web
- ouvrez les attachements de courriels avec prudence. N'ouvrez pas les attachements de sources inconnues
- vérifiez les fichiers reçus sur des disquettes, etc.

* songez à installer un coupe-feu

FAIRE FACE AU DÉSASTRE

En faisant face à un désastre, les pressions périphériques peuvent être aussi destructrices que le désastre lui-même. Considérez non seulement l'effet d'un désastre sur les systèmes physiques de votre bureau, mais aussi l'impact sur le personnel et leurs familles immédiates. Il est parfaitement normal de s'inquiéter pour sa sécurité et pour celle des autres.

Voici quelques actions à prendre :

1. Ne vous blâmez pas pour l'événement. Reconnaissez que vous serez frustré par moments à cause de votre incapacité à contrôler tout ce qui se passe autour de vous.
2. Conservez une routine aussi normale que possible à la maison et au travail. Tentez de limiter les demandes qui ne sont pas directement reliées à votre but de restauration de la normalité pour vous, votre entreprise et votre famille.
3. Même si cela ne vous paraît pas facile, essayez de partager vos sentiments avec une autre personne. La colère, la tristesse et le chagrin sont des réactions normales.
4. Demandez de l'aide, y compris d'autres avocats, avocates, et de conseillères et conseillers professionnels. Le Programme d'aide aux juristes de l'ABC est une merveilleuse ressource. Concentrez-vous sur vos forces et vos capacités.

Indices d'un besoin de counselling ou d'assistance :

- * les montagnes russes émotionnelles – facile à frustrer, sautes d'humeur, pleurer sans motif, culpabilité accablante, manque de confiance en soi, dépression, tristesse, sentiments de désespoir, nouvelles phobies (p. ex. refus de quitter son domicile, peur des foules, etc.)
- * symptômes physiques – maux de tête, douleurs d'estomac, symptômes de rhume ou de grippe, vision télescopique, sons étouffés
- * autres – difficultés de sommeil, difficulté à communiquer ses pensées, confusion, désorientation, difficulté à se concentrer et champ d'attention limité, consommation accrue de drogues et d'alcool, rendement réduit au travail et difficulté à maintenir un équilibre de vie

Aide aux employées, employés

Les employées, employés, compteront sur votre leadership et votre appui. Dans une situation de désastre qui touche à plusieurs personnes dans la même région, ils voudront partager leurs préoccupations professionnelles et personnelles. Vous voudrez sans doute envisager :

- * des avances en espèces
- * une continuation des salaires
- * des heures de travail réduites ou flexibles
- * « care packages »

- * des thérapies
- * des garderies de jour ou des services de garde

N'oubliez pas les enfants

Les enfants ne réagissent pas comme les adultes face à un désastre. Ils n'ont pas besoin d'y être exposés directement. Ils peuvent être affectés en voyant un événement à la télévision ou en entendant des adultes en parler. Les enfants peuvent à tout moment ressentir la peur, la confusion et l'insécurité.

Il est très important de répondre à leurs questions honnêtement. Ils auront besoin de beaucoup d'encouragement. Limitez les discussions de détails trop crus et assurez-vous de ne pas diminuer leur perception de sécurité. Ils vont intérioriser certaines de vos anxiétés, comme vos préoccupations financières. Essayez de maintenir une routine normale à la maison et à l'école, et continuez de participer aux activités récréatives. Réduisez temporairement vos attentes scolaires et préférez des tâches ménagères moins exigeantes.

RAPPORTS AVEC LES ASSUREURS

Informez vos assureurs

Informez les assureurs des pertes et obtenez des conseils avant d'autoriser des réparations et des dépenses d'urgence. Demandez-leur s'ils paieront pour les frais de subsistance (hôtel, buanderie, etc.) si vous êtes dans l'impossibilité de travailler et de vivre à domicile, et vérifiez si de tels versements ont un effet réducteur sur les paiements pour les dommages aux biens et l'interruption des activités du cabinet.

CONSEIL : *Il peut être opportun d'aviser votre barreau et votre assureur d'erreurs et omissions qu'il y a eu désastre et d'obtenir des conseils sur la prévention de problèmes associés aux poursuites pour négligence professionnelle (p. ex. une tombée non respectée).*

Réclamations

Conservez un registre des réparations temporaires pour prévenir des dommages additionnels, et des articles partiellement endommagés. Conservez tous les reçus, même si vous ne savez pas si la dépense est admissible (vous aurez tout de même besoin des reçus aux fins d'impôt ou de comptabilité, même s'ils ne sont pas admissibles à des fins d'assurances). Mieux vaut jeter un reçu ultérieurement que de ne pas avoir la documentation.

Advenant que vous soumettiez une réclamation pour une interruption des activités du cabinet ordonnée par l'autorité civile, conservez un registre des communications au sujet des ordres d'évacuation, y compris l'auteur de l'ordre, le temps et la date. L'évacuation d'une zone par le chef du service des incendies ou le chef de police à la suite d'un déversement chimique constitue un exemple d'une évacuation ordonnée par l'autorité civile. Vous pouvez ne pas recevoir de directive écrite ou officielle et, dans plusieurs cas, il peut s'agir d'une recommandation d'évacuer. Plus vous serez documentés, meilleures sont vos chances que votre réclamation ne soit pas rejetée. Comparez vos renseignements avec ceux d'autres entreprises touchées de façon similaire.

Faites une liste des biens endommagés (des photos et des vidéos sont recommandés) et comparez-la à votre liste avant désastre. Si vous n'avez pas de liste, vérifiez auprès des employées, employés, et des associées, associés, et utilisez d'autres sources de renseignements pour rafraîchir votre mémoire (p. ex. regardez de vieilles photos, visitez un bureau similaire, dessinez un plan d'étage, allez voir des entreprises de matériel de bureau, etc.). Vous serez surpris du nombre d'articles manquants sur votre première liste.

CONSEIL : *C'est une bonne idée de magnétoscooper tout le matériel de bureau à tous les six mois et après toute acquisition majeure, rénovation ou déménagement. Magnétoscopez le contenu de tous les tiroirs, meubles, aires d'entreposage, bureaux, placards, salles de rangement, etc. Vous serez surpris du nombre de brocheuses, de serviettes, etc. que vous possédez. N'oubliez pas les logiciels divers. Entreposez les bandes ailleurs qu'au bureau.*

Collectez tous les renseignements qui vous aideront à prouver la valeur des biens détruits ou endommagés. N'oubliez pas les sources secondaires, comme des factures, des contrats de vente, des reçus, et des relevés de cartes de crédit.

Reconstruction des dossiers perdus

Si vous n'avez pas une sauvegarde complète de tous ces renseignements, vous devrez peut-être reconstruire l'information manquante ou perdue, qui peut inclure :

- * des dossiers bancaires : rendez-vous à votre banque ou caisse, chez votre aide-comptable ou comptable. Vous recherchez des chèques, des transactions Internet, des dépôts, des bilans, des documents de prêts.
- * des renseignements sur les clients, clientes et fournisseurs : bilans, reçus, commandes, factures.
- * les services de l'impôt : les dernières déclarations et les plus récents jugements

Notification

Il est très important d'informer sans délai le personnel – c'est une étape essentielle de gestion et de contrôle. Si vous exercez un leadership, ils vous suivront. Acceptez que vous devrez chercher à gagner du temps.

Communiquez avec les clients et fournisseurs et expliquez-leur votre situation. Vous serez en mesure (selon la gravité de la situation) de remplir la plupart ou la totalité de vos engagements, même s'il faut en revoir quelques-uns.

Informez vos créanciers de délais de paiement, de factures perdues, etc. Essayez de négocier de nouveaux échéanciers de paiement, ou des réductions ou des reports de frais ou de pénalités.

Demandez à vos utilités publiques de restaurer le service le plus rapidement possible, surtout si votre bureau est inutilisable. Dans une telle situation, les paiements devraient être interrompus.

Dépôt d'une déclaration de sinistre

Rassemblez tous les renseignements sur votre police d'assurance (numéros et coordonnées des personnes ressources). Ayez recours aux services de votre agente, agent ou courtier d'assurances. Vous avez le fardeau de la preuve, en déposant votre réclamation. Vous avez donc besoin de bons renseignements et d'une documentation précise.

Discutez avec l'experte ou l'expert en sinistres du traitement de la réclamation. Demandez des paiements provisoires. Déposez une preuve provisoire de pertes. Lors de désastres majeurs, il peut y avoir des procédures spéciales. Dans certains cas, les assureurs, sur réception de la preuve d'assurance, émettent immédiatement des chèques pour un certain pourcentage des sommes assurées pour accélérer le processus de réclamation.

Voici quelques questions clés pour votre expert en sinistres ou votre agent d'assurances :

- * confirmation de l'étendue de votre couverture
- * confirmation de l'opportunité des réparations et du nettoyage que vous êtes sur le point d'entreprendre
- * préoccupations au sujet de la reprise des activités
 - quelles dépenses sont couvertes s'il faut déménager à un autre endroit
 - la couverture pour perte de revenus si vous avez dû interrompre vos activités à la suite d'une ordonnance civile
 - la couverture pour perte de revenus, même s'il n'y a pas eu de dommages ou de pertes physiques directs

CONSEIL : *Déposez votre réclamation le plus rapidement possible pour minimiser les problèmes de liquidités. Vous pourrez subir des pressions financières accrues si vous devez continuer à payer des factures pendant que votre capacité de rémunération ou de facturation d'honoraires a été réduite. Plusieurs assureurs sont prêts à offrir des paiements partiels avant le règlement final.*

Aidez l'experte ou l'expert en sinistre à vous aider. Rendez-vous disponible et donnez-lui un accès rapide et facile aux renseignements dont il a besoin. Une communication et une compréhension claires sont importantes. Fournissez une estimation provisoire des dommages et des coûts, y compris une estimation du délai requis pour un redressement complet. Aidez-les à prévoir une réserve suffisante pour votre réclamation, surtout s'il y a eu interruption des activités du cabinet.

* Faites une liste préliminaire des démarches que vous allez prendre pour une relance partielle ou complète de votre cabinet. Votre plan écrit de rétablissement après désastre vous sera très utile : en offrir un exemplaire à votre expert en sinistres créera une forte impression et aidera ce dernier ou cette dernière dans le processus de réclamation. Il ou elle verra qu'il ou elle a affaires à une personne préparée et minutieuse.

* Considérez tous les besoins financiers, y compris la masse salariale et la dette obligataire, qui auront un effet sur le cabinet durant la période de redressement.

* Conservez d'excellents dossiers des dépenses supplémentaires. Il s'agit de dépenses encourues pour accélérer la reconstruction du cabinet, y compris :

- la location temporaire d'équipement de remplacement
- les frais d'exploitation à un autre emplacement
- les frais de déménagement
- des frais spéciaux pour modifier les lignes téléphoniques, etc.

En règle générale, le calcul des pertes durant une interruption d'activités se fonde essentiellement sur une estimation à partir des dossiers historiques. Il faut s'assurer que l'estimation de la perte soit raisonnable. Certains revenus de pratique ne sont pas facilement calculés. Par exemple, si une grande partie de vos honoraires provient d'éventualités, vos revenus auront tendance à être

moins réguliers que ceux d'une ou d'un spécialiste des testaments et successions. Les documents suivants constituent de bonnes sources d'information :

- * les anciens bilans financiers – surveillez de près vos dépenses, elles ont tendance à être plus constantes d'une période à l'autre
- * les formulaires d'impôt sur le revenu
- * d'autres dossiers de pratique, des factures, des relevés de dépenses, des cartes de crédit, des renseignements bancaires

Prenez des notes durant vos conversations. Confirmez les discussions et les ententes par un suivi écrit. Comparez vos expériences et vos notes avec celles d'autres personnes dans une situation similaire.

Utilisez vos renseignements, avant et après pertes, pour vous assurer d'un règlement juste et raisonnable. S'il ne l'est pas, parlez-en à votre experte ou expert en sinistres. Si vous jugez toujours la somme offerte insuffisante, portez le règlement en appel et prenez les dispositions requises pour vous donner droit à des réclamations et à des paiements futurs.

Discutez avec votre conseiller financier de tout traitement spécial auquel vous pouvez avoir droit dans le processus de règlement des pertes.

Méfiez-vous des décisions prises dans le feu de l'action.

Engagez des entrepreneurs de bonne réputation, enregistrés auprès de la Commission des accidents de travail et possédant une police d'assurance-responsabilité. Évitez les mauvaises décisions prises dans le seul intérêt de faire évoluer le dossier plus rapidement. Obtenez des estimations de plus d'un entrepreneur et des contrats écrits.

Essayez de synchroniser vos paiements et les prestations d'assurances. Assurez-vous qu'un paiement final n'est pas exigé avant la fin des travaux. Si les pertes que vous avez subies sont répandues dans votre région, à la suite d'une inondation par exemple, il se peut que vous ayez plus de difficulté à trouver des entrepreneurs et d'autres services.

PROTECTION CONTRE LES DÉGÂTS D'EAU

Les dégâts d'eau surviennent fréquemment, et sont causés par la pluie, les inondations ou des dommages aux tuyaux. Pourquoi insister sur les dégâts d'eau ? Parce qu'il est possible de prévenir un tel incident, ou d'en réduire l'ampleur.

Les dégâts d'eau sont le plus souvent causés par des gicleurs, des inondations et de fortes pluies. Généralement, les dégâts d'eau sont très salissants et leur réparation nécessite beaucoup de travaux. Les dommages futurs causés par des moisissures ou des spores de moisissure, qui croissent rapidement dans certaines conditions et qui sont hautement toxiques, ne font qu'ajouter au problème.

Pour limiter les dégâts d'eau, il faut d'abord assécher l'édifice. Vous n'aurez pas beaucoup de succès si vous essayez d'assécher des objets pendant que la structure reste humide. Voici quelques conseils :

- * enlevez tout ce qu'il est possible d'enlever – rideaux, papeterie, etc. Il faudra peut-être enlever les tapis. Vérifiez le sous-tapis, qui agit souvent comme une éponge.
- * trouvez les endroits où l'eau a eu la chance de s'accumuler – derrière les tablettes, sous les meubles, dans les salles de rangement et les placards. Concentrez d'abord sur les endroits les plus humides.
- * assurez une bonne circulation d'air. Ouvrez les fenêtres et installez des ventilateurs et des déshumidificateurs. Vous pouvez utiliser du carton pour bâtir des souffleries simples pour diriger la circulation d'air aux endroits choisis. Essayez de maintenir la température entre 10 et 15 degrés Celsius, avec un niveau d'humidité entre 25 et 33 pour cent. N'essayez pas de chauffer avant d'avoir déshumidifié et circulé l'air.
- * couvrez les surfaces à sécher avec un papier absorbant, et changez-le souvent.

Séchage à l'air

En séchant des livres à l'air, essayez d'enlever les couvertures en plastique et insérez des essuie-tout à intervalles réguliers dans le livre, mais pas jusqu'au fond, et placez-le debout, avec le bout le plus humide en haut. S'il est impossible de le faire tenir, déposez-le à plat. N'intercalez pas toutes les pages, vous risquez de causer des dommages permanents. Changez les essuie-tout régulièrement. Plusieurs documents juridiques ont des couvertures épaisses. Dans ce cas, placez une pellicule à l'épreuve de l'eau pour empêcher l'humidité de s'infiltrer dans les pages intérieures. Vous pouvez suspendre des livres, documents, magazines et photos à une corde, à moins d'être très trempés.

CONSEIL : *En règle générale, si vous ne pouvez assécher quelque chose en 48 heures, congelez-le.*

Le papier congelé se conservera pour un maximum de six ans. La congélation commerciale par air pulsé fonctionne le mieux, à cause de sa capacité de réduire les températures rapidement. Un congélateur horizontal résidentiel avec une température de -10 Celsius est convenable pour de petites quantités de documents. À moins qu'ils ne soient extrêmement trempés, la plupart des articles de papier pourront être restaurés à un niveau acceptable d'humidité en moins de 48 heures.

Ne congelez pas des tableaux, des meubles, de la pierre, du verre, de la céramique, des métaux, des photos et des négatifs, ou des objets de bois vernis.

Généralement, les meubles peuvent être séchés à l'air. Ne frottez pas la saleté et la boue sur un meuble – il suffit de rincer et de sécher.

Plusieurs entreprises peuvent vous aider s'il s'agit d'un nettoyage à grande échelle. Elles ont accès aux équipements et aux ressources humaines requises. Vous pouvez vous occuper sans aide d'incidents mineurs.

CONCLUSION

Pour conclure, il est important de souligner quelques idées :

1. Un plan de rétablissement après désastre n'a rien de magique et ne nécessite aucune formation spécialisée. C'est comme l'exercice du droit : il requiert une analyse approfondie et de la discipline. On ne pourra jamais trop insister sur la discipline. Un plan doit être développé, consigné par écrit et testé; les utilisateurs et utilisatrices doivent le connaître et savoir comment l'utiliser.
2. Il n'existe pas de plan parfait. Chacun est différent. Personne ne peut anticiper tous les éléments d'un désastre. Un plan trop complexe a toutes les chances d'être ignoré au moment où on en aura le plus besoin. Les mises à jour seront trop lourdes et le coût de développement d'un tel plan risque d'être prohibitif. Les attributs uniques de chaque organisation entraînent des plans différents. Commencez avec un plan simple et réduite. Tout plan (même imparfait) est meilleur que l'absence de plan.
3. Le but de l'éducation, ce n'est pas d'apprendre, mais d'agir. Le but d'un rétablissement après désastre est le même – l'ACTION. C'est un appel aux armes, porteur de confiance et d'outils de leadership applicables aux circonstances les plus négatives. L'exécution de votre plan de rétablissement après désastre dépend d'un nombre de facteurs mais la preuve a été faite, à maintes reprises, qu'une bonne communication et un leadership font la différence en situation de désastre.

ANNEXE I

LISTES DE CONTRÔLE D'ÉVÉNEMENTS POSSIBLES ET DE RISQUES

La liste ci-dessous d'incidents et risques n'est pas complète, mais presque. Vous pourrez trouver que certains d'entre eux ne sont guère pertinents, ou très lointains. C'est un outil pour vous faire envisager un vaste éventail de risques, afin d'assurer une analyse et un plan plus complets.

Activité humaine (y compris l'activité criminelle)

Vol

Incendie criminel

Bombe et alerte à la bombe

Panne de logiciel (p. ex. virus, cyber-attaques et pirates informatiques)

Perte d'employées, employés, avec des tâches, des clés et des codes essentiels

Sabotage (clients, clientes, employées et employés mécontents et autres)

Émeutes et désordres publics

Guerre et insurrection

Terrorisme et prises d'otages

Perte d'accès – interruption par l'autorité civile, tempête de neige, grèves ou autres perturbations causées par les communications, le transport ou le secteur des services

Erreur humaine causée par l'insuffisance de formation, d'entretien, la négligence, l'inconduite, la toxicomanie ou la fatigue

Désastres naturels

Neige, blizzard, verglas, grêle

Tornade, ouragan et tempête de vent

Incendie de forêt

Orages violents

Inondations

Sécheresse prolongée

Séismes

Boue et glissements de terrain

Raz de marée

Éruption volcanique

Désastres d'infrastructure

Incendie ou explosion (d'une source intérieure ou extérieure)

Dommages par la fumée

Panne de courant, interruption de carburant ou d'énergie

Panne de télécommunications

Panne de serveur ou de quincaillerie

Dégâts d'eau (inondation, gicleurs)

Panne d'approvisionnement en eau

Refoulement ou panne d'égout
Pollution ou déversement chimique
Effondrement structurel
Irradiation

Accidents divers

Transport – véhicules automobiles, navires, trains, avions
Blessures corporelles
Transport de produits chimiques ou nucléaires
Bris d'aqueduc ou d'égout
Bris de lignes d'électricité ou de communications
Bris de pipeline

ANNEXE II

LISTE DE RESSOURCES D'URGENCE

Il est très important d'avoir une liste de ressources d'urgence à votre portée. Cette liste devrait inclure les services publics et privés dont vous pourriez avoir besoin. Si une ressource est essentielle, vous avez avantage à inclure des personnes ou entreprises de rechange, advenant l'impossibilité d'avoir recours à votre premier choix.

CONSEIL : *Vous serez surpris et surprise de l'utilité de cette liste, qui servira sans doute plus souvent que prévu. Les gens l'ont trouvée utile dans toutes sortes de situations qui ne tombent pas dans la catégorie des désastres.*

Coordonnées essentielles

- * numéros de téléphone
- * numéros de téléphone cellulaire
- * numéros de télécopieur
- * adresses de courriel
- * autres coordonnées (p. ex. chalet, indicatif d'appel de radio pour bateau, etc.)
- * adresses
- * la personne ressource la plus importante
- * matériel ou services fournis (s'il s'agit d'un fournisseur)
- * numéros de dossier ou de comptes, au besoin

Votre liste de ressources d'urgence peut aussi inclure :

- * service des incendies
- * ambulances
- * police
- * amis et voisins (qui peuvent offrir une assistance personnelle)
- * plombier
- * électricien
- * serrurier
- * menuisier
- * fournisseur d'électricité
- * fournisseur de gaz
- * courtier/agent (ainsi que le nom de la compagnie d'assurances et votre numéro de police)
- * autres avocats et avocats (dont l'aide peut être utile)
- * sécurité
- * propriétaire de l'édifice ou service de sécurité (au besoin)
- * personne ressource – matériels de bureau
- * personne ressource – ordinateurs
- * personnel de soutien en technologies de l'information
- * médias locaux (radio, télé, journaux)
- * autres personnes ressources (en conformité avec votre plan de rétablissement après désastre)

ANNEXE III

INVENTAIRE INFORMATIQUE

Créez un formulaire pour vos ordinateurs, périphériques et logiciels et attachez les coordonnées des fournisseurs au formulaire. Conservez une copie de cette documentation avec votre plan de rétablissement après désastre. Il est souhaitable de mettre le formulaire à jour après chaque achat important. Parmi les fournisseurs, il faut inclure les entreprises qui vous ont vendu, loué ou réparé des appareils ou logiciels. Cet outil est très utile quand vous essayez de reconstruire votre bureau. Vous pourrez plus facilement et plus rapidement déterminer ce que vous devez acheter.

Renseignements à inclure :

- * quincaillerie (p. ex. ordinateur, moniteur, imprimante, clavier, etc.)
- * information relative à la quincaillerie (p. ex. RAM, capacité du processeur, mémoire du disque dur, etc.)
- * périphériques (lecteur ZIP, modem, scanner, etc.)
- * logiciels (noter le titre, la version, les mises à jours et le numéro et le nombre des licences)
- * modèle
- * numéro de série ou numéro d'identification
- * date d'achat / location
- * coût
- * coordonnées des fournisseurs (nom d'entreprise, adresse, télécopieur, téléphone, courriel, personne ressource et numéro de compte)