

Gestion des risques

Ce que tout dirigeant d'entreprise doit savoir
pour assurer la continuité des affaires

Les technologies de l'information et des communications (TIC) jouent un rôle plus important que jamais dans le succès et même la survie de nombreuses entreprises. L'élimination des risques d'interruption des activités liés à l'infrastructure TIC fait donc désormais partie des conditions de réussite les plus déterminantes en affaires.

Depuis quelques années, de plus en plus de dirigeants d'entreprise ont compris que les risques inhérents aux affaires allaient bien au-delà des seuls sinistres. De nos jours, la planification de la continuité des affaires exige une perspective beaucoup plus vaste qui tient compte d'une série de facteurs de risque directement liés à l'efficacité des activités quotidiennes. Dans le cas des TIC, cela peut englober n'importe quelle anomalie, depuis un ralentissement du réseau ou une panne de courant, jusqu'à une défaillance des systèmes de vente en gros.

Dans le présent document, nous nous penchons attentivement sur la notion de continuité des affaires : en quoi consiste-t-elle, quelle en est la fonction et pourquoi influe-t-elle à ce point sur l'avantage concurrentiel d'une entreprise dans le contexte actuel? Nous verrons également comment une saine planification de la continuité des affaires au chapitre des TIC peut permettre d'optimiser la productivité, la sécurité et la conformité de l'entreprise aux exigences d'ordre réglementaire.

La continuité des affaires sera plus particulièrement abordée dans trois de ses dimensions essentielles :

- la sécurité de l'entreprise;
- la disponibilité maximale des systèmes de l'entreprise;
- la reprise des activités en cas d'imprévu.

Les renseignements présentés dans les pages qui suivent aideront les dirigeants à mieux comprendre la nature et la portée de ces trois dimensions, ainsi que les exigences qui en découlent en matière de continuité des affaires et les mesures à prendre pour établir un plan adapté aux besoins particuliers de l'entreprise. Il sera aussi question de gestion de l'infrastructure et de services professionnels TIC – deux ingrédients clés pour l'établissement et la mise en œuvre de processus de planification de la continuité.

La continuité des affaires est une question très présente dans l'esprit de bien des gestionnaires, dans tous les types d'entreprises. Bien que l'on entende surtout parler des grandes crises qui secouent parfois le monde des affaires, la continuité est loin de reposer uniquement sur des processus de reprise des activités après de graves sinistres. Les véritables catastrophes, d'ailleurs, ne représentent plus aujourd'hui qu'une faible part des risques inhérents aux affaires.

Selon le *Business Continuity Institute*, établi au Royaume-Uni, la gestion de la continuité des affaires s'impose désormais clairement comme une vaste discipline de gestion qui n'est plus synonyme de reprise après sinistre. Pourtant, dans l'une de ses études, l'institut révèle qu'il y a un plus grand nombre d'entreprises dotées d'un plan précis de reprise après sinistre que d'entreprises qui planifient la continuité de leurs affaires dans toutes ses dimensions.

Cependant, cette même étude relève aussi que toutes les entreprises qui disposent d'un plan de continuité des affaires ont aussi un plan de reprise après sinistre. La planification antisinistre constituant généralement une démarche assez circonscrite, elle s'inscrit en effet dans le contexte plus large du plan de continuité des affaires. Ainsi, plus on cerne les enjeux dans leur globalité, plus on règle du même coup les problèmes pointus qui en relèvent.

Les TIC occupent une place importante dans la planification de la continuité des affaires. En effet, la plupart des entreprises misent largement sur leur infrastructure TIC pour assurer leur exploitation quotidienne. Plus les données ou les applications informatiques pèsent lourd dans la bonne marche des activités, plus le soutien de l'infrastructure doit faire partie des priorités.

Les dérangements nuisibles au rendement des TIC (ralentissements du réseau, virus, pannes de courant, etc.) peuvent prendre une multitude de formes et présenter des niveaux de risque très divers.

Par exemple, même une brève interruption des systèmes intimement liés aux sources de revenus de l'entreprise risque de porter sérieusement atteinte à la rentabilité. Pensons notamment à tout ce qui touche le commerce électronique. Ce n'est cependant pas une mince tâche que de blinder l'infrastructure contre toute perturbation. Il faudrait souvent y consacrer plus de ressources humaines et financières que ne peuvent se le permettre bien des entreprises. Pourquoi la continuité des affaires présente-t-elle donc un tel défi?

Les raisons sont nombreuses. Par exemple :

- peu d'entreprises ont assez de ressources ou de compétences à l'interne pour gérer et surveiller efficacement le rendement de leurs réseaux et de leurs systèmes. De plus, les fonctions de sauvegarde quotidienne et de production de rapports peuvent s'avérer lourdes et sujettes à l'erreur humaine;
- pour assurer la résilience de l'infrastructure, il faut un centre de données spécialisé et un ensemble de processus de sauvegarde sous-jacents. De plus, la technologie garante de redondance et de résilience maximales coûte souvent trop cher, et les services TI internes des entreprises ne sont pas en mesure d'en effectuer la maintenance;
- le fardeau est de plus en plus lourd à porter pour les entreprises à qui l'on demande également de gérer et de respecter des exigences réglementaires toujours plus strictes en matière de collecte, de traitement, de stockage, de récupération et de suppression sécuritaires des données.

Selon un sondage réalisé auprès de 130 entreprises canadiennes, la sécurité arrive en tête des motifs de mise à niveau des réseaux. Deux entreprises sur trois signalent des atteintes aux mesures de sécurité de leurs systèmes ou de leurs réseaux au cours des six derniers mois, et près de 90 % d'entre elles reconnaissent l'effet néfaste de ces violations sur la productivité.

— IDC

Plutôt que de s'en tenir à une approche réactive et ponctuelle, les entreprises doivent trouver une façon souple et rentable de relever les défis auxquelles elles font face. Le prix de l'inaction peut s'avérer inabordable.

Calculer le coût des risques

Une enquête Léger Marketing révèle que 72 % des dirigeants d'entreprises canadiennes n'ont ni plan de reprise après sinistre, ni plan de continuité des affaires. De plus, selon une étude de Gartner, les deux-tiers des entreprises canadiennes ont constaté des atteintes à la sécurité de leurs systèmes ou de leurs réseaux depuis six mois. Près de 90 % d'entre elles confirment d'ailleurs que ces violations ont fait diminuer leur productivité.

Pareilles baisses de productivité se répercutent de façon variable sur les revenus et la rentabilité, selon le type d'entreprise et le niveau d'expertise interne en matière de TIC. Pour l'essentiel, les risques sont calculés en fonction de leur probabilité d'occurrence et de la gravité de leurs répercussions sur la bonne marche des affaires.

Les participants à l'étude du *Business Continuity Institute* ont fait valoir certains facteurs à considérer lorsque vient le temps d'évaluer le coût des risques. Ils relèvent, par exemple : la productivité des employés, les exigences réglementaires gouvernementales, la capacité d'attirer et de fidéliser les investisseurs, la protection des employés et l'expansion des affaires.

Pour pouvoir choisir des moyens efficaces de réduire les risques, il faut donc comprendre les facteurs et les niveaux de risque propres à l'entreprise et à son principal secteur d'activité. Plus les risques réels ou perçus sont importants, plus la planification doit être précise et permettre de parer rapidement à toute éventualité.

Continuité des affaires et TIC : les vrais enjeux

Planifier la continuité des affaires, ce n'est pas uniquement établir des processus de reprise rapide en cas d'atteinte à l'intégrité de l'infrastructure TI. C'est une vaste démarche de gestion qui transcende les considérations matérielles pour englober quantité de questions moins tangibles : la productivité des employés, par exemple, l'efficacité de la chaîne d'approvisionnement et la réputation de l'entreprise en général. Toutes ces préoccupations sont inextricablement liées à l'intégrité et au rendement des TIC.

Si l'on veut qu'elles permettent effectivement d'assurer la continuité des affaires, les solutions TIC doivent tenir compte des dimensions suivantes et en permettre la gestion intégrée :

- **la sécurité de l'entreprise** – il faut une infrastructure sécuritaire et uniquement accessible aux personnes autorisées;
- **la disponibilité maximale des systèmes de l'entreprise** – l'infrastructure essentielle doit toujours fonctionner;
- **la reprise des activités** – en cas d'imprévu, il faut des systèmes et des processus pour garantir la reprise rapide des activités.

Somme toute, une entreprise dispose d'un bon plan de continuité des affaires si elle peut affirmer sans l'ombre d'un doute que son infrastructure essentielle est sécuritaire et toujours fonctionnelle et permet d'assurer la reprise rapide des activités en cas d'imprévu.

Chacune des trois grandes dimensions de la continuité des affaires est expliquée de façon plus précise dans les sections suivantes.

La sécurité de l'entreprise

Assurer la sécurité d'une entreprise, c'est protéger son infrastructure technologique, ses données et ses applications contre les menaces externes et internes. L'objectif : réduire les risques allant du vol de renseignements à la non disponibilité des systèmes.

Parmi les enjeux prioritaires à prendre en compte :

- la protection des réseaux contre les interruptions causées par les virus, les polluriels et d'autres cybermenaces;
- l'élargissement de l'accès à l'information, de pair avec la mise en œuvre de mesures efficaces de contrôle d'accès pour les utilisateurs;
- la conformité aux exigences en matière de confidentialité des données et à d'autres exigences réglementaires telles que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) et la Loi Sarbanes-Oxley;
- la gestion stratégique et proactive du coût total de la sécurité.

On estime que 80 % des courriels envoyés en décembre 2006 étaient des polluriels.
– Globe and Mail, janvier 2007

La disponibilité maximale des systèmes de l'entreprise

Si l'on tient à assurer la disponibilité 24 heures sur 24, 7 jours sur 7 des systèmes TIC dont dépendent les activités de l'entreprise, il faut d'abord s'employer à réduire les risques et la probabilité d'interruption résultant d'un dérangement touchant le matériel, les logiciels ou les applications de télécommunications. Une partie intégrante de ce processus consiste à évaluer et à comprendre les éventuels points faibles à l'échelle d'un système intégré.

Parmi les enjeux prioritaires à prendre en compte :

- le fonctionnement ininterrompu du matériel et des applications de première importance – 24 heures sur 24, 7 jours sur 7;
- la permanence des communications entre l'entreprise et ses clients, ses employés, ses partenaires;
- le maintien de la pleine productivité des employés par la réduction des risques d'interruption touchant les PC, les applications et les périphériques;
- la conformité à la réglementation.

La reprise des activités en cas d'imprévu

Synonyme de reprise après sinistre, cette dimension clé de la continuité des affaires consiste à mettre en place des mesures pour minimiser les risques et les conséquences d'une éventuelle interruption des activités.

Selon plusieurs études récentes, jusqu'à 80 % des interruptions dans le fonctionnement des applications vitales des entreprises découlent directement d'erreurs humaines ou de processus. Les 20 % qui restent résultent de défaillances technologiques ou d'infrastructure, ou encore de sinistres.
– Gartner

Comme nous l'avons souligné précédemment, les interruptions touchant l'infrastructure TIC peuvent revêtir plusieurs formes et comporter des risques à une multitude de niveaux. Quoique rares, les catastrophes peuvent sérieusement mettre en péril le fonctionnement de l'entreprise. D'autres types d'événements moins désastreux mais plus fréquents

(défaillance de matériel ou erreur humaine, par exemple) auront parfois, eux aussi, des conséquences néfastes sur la productivité, l'efficacité et la rentabilité.

Les entreprises devraient donc se doter de stratégies de reprise de leurs activités en cas d'imprévu. Ces stratégies peuvent non seulement les mettre à l'abri de chutes de productivité et de pertes de revenus, mais aussi leur permettre de s'adapter aux changements aussi rapidement et efficacement que possible.

Parmi les enjeux prioritaires à prendre en compte :

- la poursuite des activités durant les réparations d'équipement endommagé ou défectueux;
- la récupération des données de l'entreprise qui ont été altérées ou perdues;
- la réduction à leur strict minimum des délais de pleine reprise des activités;
- l'établissement et la mise à jour régulière d'un plan de reprise – lequel peut notamment toucher des questions telles que l'accès au réseau par des responsables autorisés se trouvant à l'extérieur des établissements de l'entreprise, ou encore l'hébergement sécuritaire hors lieux des systèmes et des applications redondants.

Comment évaluer les besoins en matière de continuité des affaires?

Les exigences à respecter en matière de continuité peuvent varier de façon considérable selon le modèle d'affaires de l'entreprise et les besoins de ses employés ou de ses clients. Les entreprises qui dépendent largement du commerce électronique, par exemple, ont sans doute d'autres priorités que celles dont la santé financière dépend nettement moins de l'utilisation d'applications en ligne ou de transmission de données en temps réel.

C'est un défi colossal pour une entreprise que de vouloir répondre aux besoins de tout le monde en tout temps. La disponibilité sans faille de l'infrastructure, par exemple, peut coûter extrêmement cher et s'avérer d'une extraordinaire complexité pour une entreprise qui n'oeuvre pas dans le secteur des TIC. De nombreuses entreprises manquent tout simplement d'expertise et de ressources internes pour assurer la surveillance continue de leurs réseaux et de leurs systèmes. En outre, la reprise complète des activités en cas d'imprévu exige parfois des installations de

secours que l'entreprise ne peut pas se payer, ou dont elle n'a pas forcément un besoin immédiat.

Durant la première moitié de 2006, on comptait en moyenne 6 110 attaques par déni de service (DoS) par jour.

– Rapport de menaces de Symantec – 2006

Plus les risques réels ou perçus sont importants, plus il faut s'employer à les atténuer. Chaque entreprise est donc tenue de comprendre les risques qui la menacent, les conséquences possibles de ces risques sur des activités données, ainsi que la priorité qu'elle doit accorder à chacun d'eux. Par exemple, quelles seraient les conséquences opérationnelles d'une brève interruption des services de courriel? Le rétablissement des applications de vérification et des applications financières est-il moins prioritaire que celui des services vitaux de téléphonie IP ou d'autres services de communications?

Pour prendre les bonnes décisions, il faut avoir une idée très claire des risques propres à l'entreprise et de leur poids relatif. L'une des choses les plus importantes à faire dès le départ, c'est donc d'évaluer les risques.

L'évaluation des risques comprend ce qui suit :

- la détermination du niveau de risque, que l'on évalue en précisant les secteurs d'activité touchés par chaque type d'interruption éventuelle, brève ou moins brève, et l'établissement de catégories de risques (élevés, moyens ou faibles) en fonction de leur probabilité d'occurrence;
- la quantification du coût des risques – au-delà des coûts liés aux systèmes et au soutien, il faut tenir compte d'éléments comme les baisses de productivité, les pertes de revenus et les atteintes à l'image de marque de l'entreprise;
- l'établissement des priorités en ce qui a trait aux besoins de sécurité, de disponibilité et de reprise après sinistre;
- l'évaluation des ressources dont on dispose – infrastructure, expertise interne, budget, etc.;
- la détermination de l'investissement nécessaire pour éliminer les risques inacceptables.

Les entreprises qui manquent de ressources internes peuvent recourir aux services d'experts-conseils pour évaluer les risques auxquels elles sont exposées,

déterminer leurs zones de vulnérabilité et se doter d'un plan d'action adapté.

L'hébergement au service de la continuité

Bien des entreprises n'arriveraient sans doute pas à effectuer elles-mêmes la mise en place et la gestion d'un environnement TIC sécuritaire, totalement redondant et permettant facilement la reprise des activités ainsi que la récupération des données en cas d'imprévu. Non seulement une telle initiative coûte-t-elle très cher, mais sa complexité dépasse souvent la capacité des installations et de l'équipe TI interne.

Les services d'infrastructure d'hébergement peuvent constituer une solution intéressante en pareille situation. Il en existe plusieurs formules souples et abordables, expressément conçues pour aider les entreprises à relever des défis comme :

- la gestion de la complexité des TI;
- l'atténuation des risques d'éventuelles pannes;
- l'accroissement de la productivité;
- la réduction des coûts des TI.

En misant sur des centres de données de fine pointe et sur les services d'experts en technologies, les entreprises bénéficient de nombreux avantages par exemple : infrastructure entièrement redondante et toujours disponible, environnement sécurisé à atmosphère contrôlée, soutien jour et nuit, alimentation fiable, connectivité réseau et systèmes d'alimentation de secours.

Les entreprises ont généralement le choix d'infrastructures d'hébergement en co-implantation ou comme services gérés. La solution la mieux adaptée dépend de leurs exigences en matière de continuité des affaires, de leur budget, ainsi que de leurs ressources et de leur expertise internes.

Grâce aux services d'hébergement en co-implantation, les entreprises peuvent héberger leur infrastructure TI, en partie ou en totalité, dans un centre de données. C'est la solution idéale pour mettre l'infrastructure TI principale ou les installations de secours bien à l'abri.

Quand elles optent par ailleurs pour des services d'infrastructure d'hébergement avec services gérés, les entreprises peuvent faire appel à un spécialiste qui fournit et met en place les serveurs spécialisés ainsi que les logiciels nécessaires au bon déroulement

permanent de leurs activités. C'est alors le fournisseur qui est responsable de gérer le rendement de l'infrastructure TI, notamment l'équipement serveur, l'utilisation de la bande passante, la sauvegarde, la sécurité, les bases de données, les systèmes d'exploitation et les autres logiciels.

Les services d'infrastructure d'hébergement sous gestion peuvent aider les entreprises à :

- se doter d'une infrastructure TI de fine pointe, à un prix bien inférieur à ce qu'il en coûterait pour bâtir et gérer leur propre centre de données interne;
- réduire les risques d'exploitation en s'assurant un niveau de rendement, de sécurité et de disponibilité permanente de leurs systèmes (les garanties offertes par le fournisseur font d'ailleurs l'objet d'une entente sur la qualité du service);
- réduire au minimum la complexité et le coût de la conformité aux exigences réglementaires des gouvernements ou de l'industrie, en misant sur des processus et des technologies normalisés en matière de sécurité, de stockage et de récupération des données;
- favoriser la croissance de l'entreprise en réaffectant à des activités plus rentables les employés précédemment chargés de la gestion de l'infrastructure;
- préparer la croissance en choisissant une infrastructure évolutive, en mesure de prendre de l'expansion rapide et selon les besoins.

Les entreprises qui souhaitent héberger leur propre infrastructure, mais à qui certaines compétences font défaut en matière de soutien TI, peuvent également se prévaloir de services de gestion à distance. Ceux-ci prévoient notamment la surveillance à distance et le soutien technologique 24 heures sur 24, 7 jours sur 7 de tous les éléments de leur infrastructure –serveurs, réseaux locaux, postes de travail, imprimantes, dispositifs de sécurité, installations de secours, etc.

Trouver les bonnes ressources

Dans l'environnement concurrentiel d'aujourd'hui, la planification de la continuité des affaires est essentielle à la survie des entreprises. Lorsqu'il est question de rentabilité et de rendement général, il est important de comprendre que ce ne sont pas toujours les sinistres les plus visibles ou dramatiques qui font le plus de dommages. Même les interruptions mineures mais fréquentes résultant d'erreurs internes, d'une mauvaise utilisation des systèmes, de virus, d'une

infrastructure instable ou de retards dans la prestation du soutien technique exigent souvent de lourds investissements humains et financiers susceptibles d'entraîner une hausse significative des coûts et une baisse de la productivité de l'entreprise.

Pour éviter de tomber dans le piège des dépenses inutiles et inefficaces, les dirigeants d'entreprise doivent d'abord prendre l'engagement de se doter d'un plan de continuité des affaires. Cet engagement ouvre la porte aux démarches essentielles d'évaluation des risques et de leurs éventuelles répercussions, de mise en priorité des besoins de l'entreprise et de mise en œuvre des mesures propres à assurer la continuité des affaires.

Une étude indique que 72 % des dirigeants d'entreprises canadiennes n'ont établi ni plan de reprise après sinistre, ni plan de continuité des affaires.

– Léger Marketing

Les entreprises qui ne possèdent pas toutes les ressources voulues ont la possibilité de se prévaloir d'une foule d'offres de services experts en TIC pour obtenir le soutien dont elles ont besoin. Les solutions à leur disposition peuvent les aider à réduire les risques opérationnels et les coûts connexes, tout en améliorant leur productivité et leur rendement d'ensemble.

Le plus important, c'est de trouver des fournisseurs experts en matière d'évaluation des risques et de leurs conséquences sur les activités de l'entreprise, et de soutien des infrastructures et des systèmes. Pour mettre les TIC au service de la continuité des affaires, il faut en effet de multiples compétences dans plusieurs domaines de pointe ainsi qu'une infrastructure de classe mondiale. Comme nous l'avons expliqué ci-haut, il s'agit aujourd'hui d'une discipline à part entière. Les entreprises devenant de plus en plus dépendantes de leur infrastructure TIC, elles ne peuvent plus assurer leur avenir, ni même leur réussite immédiate, sans un partenaire à long terme capable de leur procurer tous les services essentiels à la continuité de leurs affaires.

Les solutions de Bell en matière de continuité des affaires

De plus en plus d'entreprises arrivent à éliminer les risques d'interruption de leurs principales activités en

confiant à Bell la protection de leur infrastructure TIC. Bell offre en effet une gamme complète de services professionnels d'évaluation, de planification des infrastructures TIC, d'approvisionnement, de mise en œuvre et de gestion. Ces services peuvent aider les entreprises à assurer :

- **leur sécurité globale** – celle de leur infrastructure, de leurs données, de leurs applications et de l'accès à leurs systèmes et à leurs réseaux;
- **la disponibilité maximale de leurs systèmes et la permanence de leurs activités** par le soutien 24 heures sur 24, 7 jours sur 7 du matériel et des applications TIC;
- **la reprise rapide de leurs activités en cas d'imprévu**, grâce aux ressources de secours nécessaires et dans le respect des exigences de confidentialité des données.

Les solutions de Bell offrent aux entreprises des choix abordables et souples qui facilitent la gestion et la maintenance internes des systèmes tout en soulageant les équipes TI d'une partie de leurs responsabilités les plus stressantes et les plus accaparantes. Elles comprennent notamment :

Les services professionnels

Il s'agit d'une gamme de services – comme l'évaluation de la vulnérabilité, l'analyse de l'impact, la planification de la continuité et reprise des activités – qui aident les clients à cerner et à comprendre leurs besoins en matière de continuité des affaires.

Les services d'infrastructure

De l'approvisionnement en matériel et en logiciels à l'installation, à la maintenance et au soutien, les services d'infrastructure aident les entreprises à se tenir au fait de leurs besoins technologiques en matière de sécurité, de disponibilité maximale et de reprise des activités.

Les services de gestion

Les services cogérés et les services entièrement gérés sont conçus pour optimiser la sécurité, l'efficacité, la performance et la disponibilité de l'infrastructure d'information et de communications d'une entreprise, tout en réduisant la complexité, les risques et les dépenses d'investissement.

L'avantage Bell

Bell est l'un des fournisseurs de solutions TIC les plus expérimentés du pays. Parmi les avantages décisifs qu'elle vous procure :

Expérience et fiabilité

Depuis plus de 125 ans, Bell fournit des services de communications fiables à la population et aux entreprises canadiennes. L'efficacité de nos solutions TIC découle notamment d'investissements considérables dans des infrastructures clés, dont un centre de données et un réseau IP d'envergure nationale.

Expertise reconnue

Notre équipe chevronnée de professionnels multidisciplinaires comprend l'évolution de la technologie. Elle a déjà largement fait ses preuves en livrant des solutions de continuité des affaires aux entreprises d'ici.

Création de valeur

Bell offre un ensemble hors pair de services en matière de sécurité, de continuité des affaires, de reprise des activités en cas d'imprévu et de conformité aux exigences réglementaires. Avec le concours actif de partenaires clés de l'industrie, elle constitue pour vous un véritable guichet unique pour tout ce qui touche l'évaluation, la conception, la mise en œuvre, l'intégration et la gestion, quels que soient vos besoins présents et futurs en matière de services TIC.

Pour plus de renseignements, communiquez avec votre conseiller de Bell ou votre partenaire certifié de Bell.

bell.ca/continuitedesaffaires

