Dossier

De la gestion

par Linda Ducret
et Patrick Brébion

La gestion des nouveaux risques

Quels sont les risques existants en entreprise ?

- La prévention des risques est l'affaire de tous

Les nouveaux dangers passés en revue

- Risques informatiques, risques liés à la mobilité, risques liés au Cloud Computing, risque d'image et de e-réputation, risques psychosociaux, risque environnemental, risque produit

Pourquoi gérer ces nouveaux risques ?

- Seule une stratégie globale des risques bien maîtrisée et régulièrement actualisée, permet de gérer le développement de l'entreprise et d'assurer sa pérennité.

Comment gérer ces risques ?

- La gestion du risque informatique figure en tête des périls majeurs pour les entreprises.

Sécuriser les outils de mobilité

État des lieux des risques de la mobilité

- 3325 % d'augmentation du nombre de logiciels malveillants ciblant Android OS au cours des 7 derniers mois 2011

Les solutions

- La meilleure alternative est de gérer les smartphones comme les autres équipements informatiques et, mieux, d'intégrer cette gestion dans la sécurité du système d'information.

Protéger ses documents sensibles

Sécuriser les systèmes d'information

- Confier en ligne ses documents sensibles à des sociétés spécialisées est désormais une véritable alternative

La facture électronique et le risque fiscal

- Sous réserve du respect des conditions indiquées dans ces textes, une entreprise n'est plus tenue d'émettre des factures sur papier, la facture « immatérielle » étant alors reconnue comme un original.

intelligente des risques

« Connaître son ignorance est la meilleure part de la connaissance », dit un proverbe chinois.

Le dirigeant d'aujourd'hui ne peut plus ignorer les risques et ce d'autant qu'ils interagissent entre eux et menacent en permanence son entreprise.

Quels sont les risques existants en entreprise ?

La prévention des risques est l'affaire de tous ceux qui travaillent au sein de l'entreprise. Encore faut-il identifier ces risques et savoir pourquoi et comment les gérer. La rédaction de *GPO Magazine* vous invite à les décrypter à travers un questionnement sur les risques présents dans l'entreprise, la nécessaire prévention et le développement d'un système de protection au sein de la structure.

La prise de risque est au cœur de l'entreprise : en effet, force est de constater que le risque est inhérent à la fonction du dirigeant et que sa gestion fait partie de ses missions. Dans les grandes sociétés il existe désormais, au niveau du siège, un professionnel à temps plein pour coordonner la démarche de gestion des risques dans sa totalité. Les PME, quant à elles, ne peuvent plus faire l'économie de la gestion des risques. Cependant, le processus peut apparaître complexe car leur nombre est croissant. Si les dangers classiques sont toujours présents et bien connus (risques financiers, sociaux, humains, technologiques, de production, de commercialisation, opérationnels, politiques...), des périls nouveaux ont émergé tels que ceux liés à la mobilité, à l'informatique (piratage, perte de données), à l'émergence du *cloud computing*, à l'image et à l'e-réputation. Sans oublier les risques psychosociaux, environnementaux, et risques produits liés à la réglementation.

La prise de risque est au cœur de l'entreprise. Les PME, quant à elles, ne peuvent plus faire l'économie de la gestion des risques

Les nouveaux dangers passés en revue

FrontGRC

▶ **Un exemple de programme de gestion des risques en entreprise**

FrontGRC est une solution intégrée pour la gouvernance d'entreprise, la gestion des risques et la conformité. Elle permet aux entreprises de répondre à leurs obligations règlementaires (exemples : Bâle II et Bâle III pour les banques, Solvabilité II pour les assurances). Avec FrontGRC, les entreprises peuvent optimiser leur organisation et leurs processus et ainsi atteindre les objectifs financiers et stratégiques fixés. FrontGRC offre les fonctionnalités suivantes :

- L'identification des zones à risques de l'activité de l'entreprise (cartographie des risques, collecte des incidents)
- La mise en œuvre d'un dispositif de contrôle (contrôle permanent et contrôle périodique, audit interne
- La mise en œuvre et le test de plans de continuité d'activité. ■

• **Risques informatiques** : les menaces sur le capital informatique d'une entreprise n'ont jamais été aussi grandes. Bien entendu, un sinistre électrique, un incendie, une erreur de manipulation, une panne matérielle peuvent affecter le système informatique d'une entreprise. Mais les attaques ou destructions d'un tel système peuvent également mettre à genoux n'importe quelle entreprise, y compris une multinationale.

• **Risques lié à la mobilité** : au début des années 2000, les responsables de la sécurité des systèmes d'information ont dû gérer la préférence exprimée par de nombreux cadres pour des ordinateurs portables. Car avec la mobilité sont apparus de nouveaux dangers tels que le risque de vol ou de pertes de données sensibles, ou encore d'intrusion dans le système d'information de la collectivité, *via* l'Intranet.

• **Risques lié au *cloud computing*** : côté face, il y a des ressources informatiques flexibles et disponibles sans limites géographiques, une absence de gestion des mises à jour, etc. Côté revers de la médaille, il y a des risques de vol de données et de dépendance vis-à-vis d'un prestataire.

• **Risque d'image et de réputation** : le dirigeant sait désormais que son entreprise (sa marque, son action) peut, à tout moment, subir un « crash de réputation » qui aura des conséquences lourdes, à l'instar d'un crash financier, dans la mesure où dans la réputation réside une partie de la création de valeur.

• **Risques psychosociaux** : troubles de la concentration, du sommeil, dépression... Un nombre grandissant de salariés déclare souffrir de symptômes liés aux risques psychosociaux. Le phénomène n'épargne aucun secteur d'activité. Indépendamment de leurs effets sur la santé des individus, les risques psychosociaux ont un impact sur le fonctionnement des entreprises (suicide, absentéisme, *turnover*, ambiance de travail...).

• **Risque environnemental** : les entreprises peuvent être à l'origine d'un risque pour l'environnement sans pour autant subir des sanctions financières. Inversement, elles peuvent se trouver exposées à un risque financier alors que la menace qu'elles font courir à l'environnement est négligeable. En effet, force est de constater qu'une entreprise peut perdre des clients si ses déficiences sur le plan environnemental sont révélées au grand jour. En justice, la condamnation pour le déversement de déchets toxiques peut peser lourd sur son bilan. Enfin, sur le plan réglementaire, les autorités peuvent augmenter ses coûts opérationnels ou, ultime décision, rendre impossible l'exercice de toute activité.

• **Risque produit lié à la règlementation** : au-delà de la prévention des risques professionnels, les entreprises utilisatrices de produits chimiques doivent également respecter ou mettre en œuvre certaines obligations ou règles de protection de l'environnement.

Intégrer les risques psychosociaux dans le document unique

Voila qui mérite quelques explications. Si on commence à savoir ce qu'est le document unique en matière de risques au travail, on sait beaucoup moins qu'il englobe les troubles psychiques. Pourtant, la responsabilité des chefs d'entreprise à cet égard est identique. Au départ, on trouve le cadre réglementaire du décret de 2001 créant le DUER (Document unique d'évaluation des risques) que chaque entreprise se doit de réaliser. Afin de prévenir les accidents du travail et les maladies professionnelles, l'entreprise doit en effet en rechercher les facteurs et les inscrire dans le document mis a la disposition du personnel. Parallèlement, elle doit, avec une obligation de résultat, mettre en place un programme annuel de prévention des risques identifiés dans le document.

La santé, y compris mentale

Trop peu d'entreprises savent que les risques dits « psychosociaux » sont explicitement intégrés aux risques professionnels. Le Code du travail fait ainsi obligation aux employeurs d'assurer la sécurite et la santé de leurs salariés (art. L.4121-1 du Code du travail). Cette obligation englobe aussi la santé mentale et psychique. ■

Source : Intégrer les risques psycho-sociaux dans le document unique, 28/02/2011, industrie-hoteliere.com

Trois questions à

Paul-Vincent Valtat, «Il faut absolument que les PME se préoccupent de l'environnement »

Paul-Vincent VALTAT
Président de la commission Environnement, Santé et Sécurité de l'Amrae

Prévenir le risque environnemental est-ce une nécessité pour toutes les entreprises, y compris les PME et n'est-ce pas un coût trop important pour une PME ?

> Il faut absolument que les PME se préoccupent de l'environnement. Pour nombre d'entre elles, recruter un *Risk Manager*, acteur majeur de la prévention des risques, peut apparaître financièrement difficile. Mais le management global des risques peut être porté par un secrétaire général, un directeur financier ou juridique ou industriel... L'Amrae a tout un ensemble d'outils et de formations pour les aider dans cette démarche.
Gérer les risques, notamment environnementaux, est non seulement une obligation légale mais aussi une source d'économies. Quand une société dispose d'une réelle pratique de prévention et de gestion des risques, les primes d'assurances baissent automatiquement. Mais aussi, prévenir le risque environnemental permet d'accéder à des marchés pour lesquels des certifications de type Iso 14001 ou des systèmes de management environnemental sont des prérequis.

Comment prévenir ce risque ?

> Le risque environnemental, comme tous les autres, doit être débusqué en amont. Il convient d'abord d'identifier les risques environnementaux en établissant leur cartographie. Il reviendra ensuite au management d'organiser et de mettre sur pied une mission de protection adaptée au budget de l'entreprise et à la réalité des menaces ainsi qu'aux enjeux. L'Amrae et L'Orée éclairent les industriels sur ces questions.

Pour vous, est-il préférable de se protéger en amont contre ce risque ou de contracter une assurance ?

> Ce n'est pas l'un ou l'autre, mais l'un et l'autre. Le *Risk Management*, c'est permettre à l'entreprise de mener sa stratégie dans une prise de risques maîtrisés. L'assurance participe de cette maîtrise. Le directeur général va conduire l'entreprise dans un cadre de risques connus et maîtrisés. C'est à lui qu'il revient d'identifier, de quantifier et de faire réduire ces risques par ceux qui en sont « propriétaires », c'est-à-dire les opérationnels. Les risques résiduels étant transférés à l'assurance. ■

Sources : AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise)
Orée, association multi acteurs créée en 1992

Pourquoi gérer ces nouveaux risques ?

Un constat : à peine la moitié des entreprises françaises évaluent l'ensemble de leurs risques tous les ans. Or les experts sont formels : seule une stratégie globale des risques, bien maîtrisée et régulièrement actualisée, permet de gérer le développement de l'entreprise et d'assurer sa pérennité. C'est dire que les nouveaux risques, tout comme les anciens, doivent être préalablement identifiés et gérés, sous peine de mettre en danger l'entreprise. En effet, les risques peuvent altérer gravement sa performance. Il faut donc comprendre et prévenir ces risques avant les autres afin de ne pas perdre un avantage concurrentiel. *« L'entreprise s'aperçoit que l'intelligence des risques devient un facteur de performance et une mine d'avantages concurrentiels lisibles »* soulignent Bernard Besson et Jean-Claude Possin[1]. Plus que jamais, la prévention doit être le maître-mot. *« Car le temps et l'argent consacrés à entrevoir l'occurrence de risques seront toujours infiniment moindres que le temps et l'argent dépensés pour en réparer les dégâts »* précisent ces deux grands spécialistes de l'intelligence des risques. De son côté, Gildas Mathurin, COO Front GRC et Business Solution met en avant la nécessité de mettre en œuvre des procédures internes afin de faire face à des risques potentiels ou avérés de non-continuité des activités : *« Quelle que soit la typologie des risques, il est essentiel de mettre en place des solutions pour que l'entreprise ne soit pas fragilisée. En tant qu'éditeur de logiciels, notre approche globale est de proposer des outils innovants permettant de poursuivre l'activité de l'entreprise. C'est pourquoi celle-ci doit se doter d'un plan de continuité pour maintenir la qualité de ses services en cas de circonstances exceptionnelles telles que les catastrophes naturelles, les pandémies, les défaillances techniques importantes ou encore le terrorisme ».*

Gildas MATHURIN
COO Front GRC et Business Solution

> *« Quelle que soit la typologie des risques, il est essentiel de mettre en place des solutions »*

La gestion du risque informatique est en tête

Elle est étroitement liée à la stratégie des entreprises. « *En effet, gérer une entreprise, ce n'est ni*

Thierry CHIOFALO
RSSI (Responsable de la sécurité des systèmes d'information) et membre du Clusif (Club de la Sécurité de l'Information Français)

> *« Il est donc essentiel pour l'entreprise de contrôler le risque lié à l'usage des systèmes d'information »*

plus ni moins que de prendre des décisions en fonction de risques de gains ou de pertes. Au cours de dernières années, l'utilisation des systèmes d'information s'est de plus en plus généralisée, permettant ainsi d'améliorer les process de l'entreprise grâce à l'automatisation des flux d'information. Celle-ci a en général permis d'accélérer les traitements et de diminuer les erreurs humaines. Ainsi, aujourd'hui, tous les process d'une entreprise, qu'ils se rattachent à une fonction de soutien ou de production, ont une dépendance forte au système d'information. Il est donc essentiel pour l'entreprise de contrôler le risque lié à l'usage des systèmes d'information, dans la mesure où la création de la valeur ajoutée de l'entreprise est de plus en plus dépendante de ces systèmes » souligne Thierry Chiofalo, RSSI et membre du Clusif.

Le risque d'atteinte à l'image et à la réputation

Tout simplement parce ce qu'il est considéré comme la conséquence potentielle de tous les autres types de risques. *« Les facteurs les plus structurants de la réputation d'une entreprise sont les produits, la gouvernance et la citoyenneté. En fait, les composantes du risque de réputation et d'e-réputation sont nombreuses et passent aussi par les procès (SGale - Kerviel), l'image des dirigeants (rémunération excessive de l'ancien PDG de Vinci) ou encore l'innovation (Freebox Révolution de Free, Vehicule Electrique Autolib de Vincent Bolloré). Autant de facteurs, qui, s'ils sont évoqués sur Internet dans des articles de presse, blogs, avis consommateurs « font » la réputation de l'entreprise »* indique Christophe Asselin, Expert veille et e-réputation chez Digimind.

Comment gérer ces risques ?

Il existe une multitude de risques : c'est pourquoi le premier réflexe doit être d'en établir une hiérarchie. Certains sont acceptables, d'autres non. Il y a lieu d'établir une stratégie qui doit être définie et retenue par la direction de la société après avoir préalablement consulté les différents conseils de l'entreprise tels que l'avocat, l'assureur, le comptable...

Comment gérer le risque informatique ?

« La gestion du risque lié au système d'information peut être abordée de deux façons complémentaires : la sécurisation systématique ou l'analyse. La sécurisation systématique consiste à mettre en place un ensemble de mesures regroupées en « bonnes pratiques » dont la finalité est de réduire le risque ou ses conséquences. Dans la vie courante, cela reviendrait à s'assurer que toutes les portes ont des serrures et que le local est bien assuré contre les conséquences du vol. L'analyse du risque consiste à identifier les différents dangers et leurs conséquences afin d'évaluer le bien-fondé éventuel de solutions de protection. Pour reprendre l'exemple de la vie courante, cela consisterait à enquêter sur les statistiques de cambriolage pour savoir si le risque existe à l'endroit où se trouve le local. Ici, il s'agit non pas de se protéger forcément mais d'avoir conscience du risque pris et des possibilités de réduction de celui-ci afin de pouvoir exercer son choix. Une seule de ces deux façons de gérer serait peut-être problématique eu égard à la finalité qui est de préserver la chaîne de valeur : l'application de bonnes pratiques systématiques à un niveau important peut amener à se surprotéger, et mener une analyse détaillée sur le périmètre complet d'une entreprise serait excessivement long et coûteux, voire irréalisable. Si par le passé un certain nombre d'entreprises se sont contentées de la mise en œuvre de bonnes pratiques (« de fermer les portes »), la maturation de ces organisations dans le domaine de la gestion des risques les ont progressivement amenées à développer l'analyse de risque. La gestion du risque va alors consister à la mise en place d'une sécurité minimum par le biais de bonnes pratiques, et à développer par ailleurs une analyse permettant de fournir un outil de décision pour les risques importants, et qui pourra résulter en l'ajout de pratiques complémentaires. » précise Thierry Chiofalo.

Christophe ASSELIN
Expert veille et e-réputation chez Digimind

> *« Éteindre le départ de feu sur le web, via un dialogue et des réponses argumentées, est une bonne solution mais ce n'est pas une science exacte »*

Qu'en est-il du risque d'image ?

Il convient notamment de surveiller et d'analyser les conversations à propos de vos dirigeants, produits, marques, et sur votre entreprise en général pour anticiper un risque d'atteinte à la réputation plus important. Ainsi, par exemple, si des internautes se plaignent de votre politique RH ou de vos produits, et que cela provoque un *buzz* durable sur Internet, l'information peut être reprise par des sites web ayant de plus en plus de visibilité pour finir sur les Mainstreams medias (TV, presse écrite) *« Éteindre le départ de feu sur le web,* via *un dialogue et des réponses argumentées, est une bonne solution mais ce n'est pas une science exacte. Digimind propose de surveiller et d'analyser, grâce à son logiciel, tout ce qui peut se dire à propos de votre entreprise tels que les publications d'articles, d'études, de billets de blogs, de forums, de tweets, de posts Facebook, de vidéos etc... bref de tous les formats web. Si votre produit ou marque se trouve cité, vous êtes alertés en temps réel »* souligne encore Christophe Asselin. ■

Linda DUCRET

1. Source : *L'intelligence des risques*, Bernard Besson et Jean-Claude Possin, Éditions IFIE

Blackberry, IPhone, IPad... Attention danger !

Si les avantages des terminaux mobiles sont incontestables, ces derniers sont souvent utilisés professionnellement sans être sécurisés. État des lieux des risques et des solutions.

État des lieux des risques de la mobilité

3325 % au cours des 7 derniers mois 2011. C'est l'augmentation du nombre de logiciels malveillants ciblant Android OS, un logiciel équipant une bonne part des smartphones. Voilà pour les chiffres récemment publiés[2] par Juniper Networks, une société spécialisée dans la sécurité. Des dangers qui se matérialisent sous des formes tout-a-fait concrètes et ont des conséquences sonnantes et trébuchantes. Des applications logicielles « infectées » composaient par exemple des numéros surtaxés, à l'insu de l'utilisateur, ou récupéraient certaines données d'identification. Les autres logiciels systèmes équipant les terminaux mobiles, BlackBerry OS, Windows Mobile et Symbian, ne sont pas à l'abri. Ces trois plates-formes sont régulièrement victimes de « malware » qui, entre autres, peuvent effacer, lire les SMS, ou encore éteindre et allumer l'appareil. En outre, les terminaux mobiles utilisés en entreprise embarquent de plus en plus souvent des applications logicielles métier. Ces dernières permettent par exemple d'accéder ou de mettre à jour des stocks, des commandes, des données commerciales, etc. Pour s'adapter aux contraintes techniques des smartphones, notamment pour le formatage des données, ces applications ne respectent pas toujours la même sécurité que pour les PC. Conséquence, « *le risque majeur est que ces applications sont des tunnels directs entre l'application mobile et le cœur du système d'information des entreprises (bases de données, annuaires, services web, etc.)* », souligne Matthieu Estrade, directeur technique de Bee Ware et spécialiste en sécurité informatique.

En savoir plus

Mobility for Business

10 & 11 octobre 2012
Cnit – Paris La Défense

L'événement des solutions et applications mobiles pour les entreprises

Les solutions pour sécuriser les outils

Comme un PC

La première étape est d'utiliser la sécurité incluse dans les terminaux mobiles. À savoir, ne pas laisser les mots de passe par défaut et mettre à jour les versions de logiciels systèmes proposées par le constructeur. Ces dernières corrigent souvent des problèmes de sécurité. Autre aspect, à l'instar des PC, les smartphones, Blackberry, iPhone, iPad, etc. contiennent souvent des informations importantes comme un courriel de confirmation d'un client par exemple. Il importe donc de les sauvegarder. Une opération qui prend la forme d'une synchronisation manuelle avec un ordinateur. Des logiciels spécifiques, appelés utilitaires, sont disponibles pour chaque famille de terminal. Par exemple, le logiciel BlackBerry Desktop Software pour les BlackBerry ou encore Android OS qui permet de synchroniser les données de son smartphone avec ses applications comme Google Contacts. Des applications de

2. Source : www.juniper.net

Des risques juridiques aussi

Interview

Sherley BROTHIER
Directeur R&D de Keynectis

« La tendance « Bring Your Own Device » est aujourd'hui un enjeu technique, économique mais également social reconnu par tous. Pourtant, la prise en compte du BYOD dans le système d'information n'est pas aussi évidente que cela peut y paraître, notamment parce que l'équipement est acheté par le salarié lui-même (sans financement de l'entreprise). En effet, dans ce contexte, l'utilisateur devra obligatoirement donner son accord pour changer un paramétrage, pour installer des logiciels de sécurité, pour disposer de la fonctionnalité d'effacement à distance ou encore pour activer les fonctions de géolocalisation. Dans ce modèle, ce n'est plus l'entreprise qui décide mais bien l'utilisateur... Pour la plupart des entreprises la tendance BYOD est prise en compte sous un angle exclusivement technique alors que le phénomène pose également des questions juridiques et sociales. On notera, par exemple, que rien n'interdit à un salarié de travailler autant qu'il le désire sur son temps libre, mais il lui est par contre strictement interdit de s'occuper sans limite de tâches personnelles sur son temps de travail ». »

sauvegarde comme Sprite Backup (www.sprite-software.com) permettent de se connecter à des services de sauvegarde en ligne comme Dropbox ou Box.net. Pour les appareils sous Windows Phone 7, Outlook Hotmail Connector transfère les adresses de messagerie, calendrier, contacts sur un compte Windows Live.

Précautions d'usage

Au quotidien, l'utilisation de smartphones sur les réseaux sans fil, wifi ou *bluetooth*, fait courir un risque certain. Privilégier les réseaux cryptés ou, au moins, sécurisés par mots de passe est conseillé, de même que désactiver les fonctions sans fil lorsqu'elles ne sont pas nécessaires. Autre recommandation, il est préférable de masquer le numéro de téléphone lorsque le destinataire n'est pas identifié. Pour limiter les risques, les éditeurs d'antivirus et autres solutions de sécurisation proposent des outils spécifiques pour les smartphones. On peut citer Bee Ware avec sa plateforme i-Suite. Avast a décliné ses outils pour les smartphones. Avast Free Mobile Security est une application gratuite pour les Smartphones sous Android. Elle dispose de fonctions spécifiques gérables à distance. Ces dernières protègent les utilisateurs des menaces en ligne et de la perte ou du mauvais usage de leur appareil. F-Secure Mobile Security, qui fournit les dernières mises à jour de sécurité pour les téléphones Android et les tablettes, peut être achetée sur Google Play. De nombreux autres éditeurs proposent des solutions spécifiques. Par exemple, MobilityGuard, AirWatch, distribué en France par Interdata, etc.

Intégrer dans le système d'information

La meilleure alternative est de gérer les smartphones comme les autres équipements informatiques et, mieux, d'intégrer cette gestion dans la sécurité du système d'information. Avec quelques spécificités cependant. Les smartphones sont souvent achetés par les salariés sur leur propres deniers, dans la moitié des cas si l'on en croit une étude[3] de l'Ifop réalisée pour le compte de la société Good Technology. Il faudra donc distinguer les données personnelles des professionnelles. Une fois ce point réglé, les terminaux peuvent être complètement intégrés dans la gestion de la sécurité de l'entreprise. Des éditeurs proposent des solutions communes permettant de sécuriser les terminaux mobiles comme les PC, tablettes, etc. Par exemple, avec MobilityGuard, l'utilisateur se connecte de n'importe où et avec n'importe quel appareil (PC, tablette, smartphone etc.), s'identifie une seule fois et a accès à tous les services autorisés. Tous ces investissements se justifient bien sûr au regard des risques encourus. Mais le constat est simple, dans la plupart des cas, ni les terminaux mobiles, ni les informations qu'ils contiennent ne sont sécurisés alors que des solutions existent. ■

Patrick BRÉBION

3. Source : www.slideshare.net


© goodluz - Fotolia

Protéger ses documents sensibles

Pour pallier aux problèmes informatiques, confier en ligne ses documents sensibles à des sociétés spécialisées est désormais une véritable alternative. À condition de vérifier quelques points...

Sécuriser les systèmes d'information

Perdre ses factures fournisseurs, ses bons de commande... quel dirigeant n'a pas eu cette peur un jour ou l'autre ? Le risque était déjà présent du temps du « tout papier ». Un incendie pouvait faire disparaître une entreprise. À ce jour, l'informatisation n'a pas vraiment diminué ce risque. Elle s'est banalisée dans l'entreprise sans que la sécurité suive. En outre, les pannes de disques durs et autres « bogues » sont beaucoup plus courants que les incendies. Des problèmes plus souvent liés à des maladresses et à des malveillances internes qu'à des réseaux de *hackers*. Selon un rapport du Clusif[4], les entreprises interrogées signalent que 37 % des incidents de sécurité informatique concernent un vol ou une perte de matériel, contre 8 % pour les intrusions sur les systèmes d'information. Toutes les organisations, même les plus sensibles, sont concernées.

Le maillon faible, l'humain...

« *Lorsqu'il s'agit de la gestion des informations, l'élément humain est le plus souvent le maillon faible de la chaîne* », déclare Florian Kastl, directeur International du Département de la Sécurité, de la Sûreté et de la Continuité d'Activité de Iron Mountain. « *Les informations sont le cœur de l'entreprise et il est vital que les sociétés mettent en place des contrôles stricts leur permettant de réduire, voire de prévenir, le risque de vols par leurs employés* ». Le danger interne est d'autant plus difficile à contrôler qu'il n'implique pas forcément la malveillance. Emporter un fichier pour continuer à travailler de chez soi, sur son PC familial non sécurisé, n'est, à priori, pas répréhensible mais peut déboucher sur la perte de données ou leur corruption par un virus. Dans un registre plus malveillant, des salariés peuvent à la veille de leur licenciement accéder au serveur, *via* un web café, et emporter des données confidentielles.

Externaliser, une alternative crédible

La première réaction, sécuriser son système d'information, est naturelle. Mais, pour être exhaustive, cette démarche se décline sous de multiples formes et devient vite compliquée et onéreuse. Par exemple, la mise en place d'un plan de reprise d'activité informatique implique des investissements lourds. Il s'agit, entre autre, de répliquer les informations sur un site distinct du site principal de l'entreprise. Si elle n'évite pas de sécuriser à minima son système d'information, utiliser les services d'une société spécialisée est une alternative. Cette dernière est devenue crédible depuis quelques années avec la banalisation du haut débit et la maturité des technologies de sauvegarde et d'archivage. Quelques banques, BNP Paribas, le Crédit de Bretagne, etc. utilisent déjà ce type de services.

Plusieurs niveaux de services

Le principe de base de ces offres est à peu près toujours le même. Les documents numériques,

4. Clusif (Club de la Sécurité de l'Information Français

Jean-Marc RIETSCH
Président de la Fedisa

« *Il faut apporter la preuve de l'intégrité des documents tout au long de leurs parcours, de la création à l'archivage* »

factures au format pdf ou scannées à partir du papier par exemple, sont envoyés par Internet (email, ftp, service web) au prestataire. Ce dernier se charge de sécuriser le stockage et de donner un accès en ligne aux documents. Directeur Général de la société Opus Conseil, Jacques Leret distingue « *quatre niveaux de services d'archivage dans une offre telle que Arkansaas* ». Le premier niveau correspond à de la sauvegarde. Le second à de l'archivage économique ; il inclut quelques fonctions supplémentaire comme, par exemple, la possibilité de gérer son plan de classement pour retrouver facilement ses documents. Un troisième niveau est souvent baptisé coffre-fort électronique ; outre les possibilités de gestion, il inclut les technologies garantissant la valeur probante des documents comme la signature électronique et l'horodatage, ce qui fait la différence en cas de litige. Le dernier cas de figure recouvre un véritable système d'archivage électronique, dans ce dernier cas, « *le nombre de documents concernés comme leur importance justifient d'intégrer l'archivage dans l'ensemble du système d'information, en particulier dès la création de documents sensibles* ».

Une offre du marché pléthorique

L'offre du marché est surabondante. La sauvegarde est souvent opérée dans des salles blanches, comprenant de nombreux serveurs informatiques et sécurisés. Le prestataire prend souvent en charge le logiciel permettant de verser et d'accéder aux archives. Côté acteurs, on trouve aussi bien des entreprises informatiques qui proposent de la sauvegarde en ligne que des spécialistes de la sécurité informatique. Dans cette jungle, se démarquent les « *pure players* » qui ne proposent que cette prestation, et les entreprises pratiquant l'archivage papier mais qui ont ajouté le numérique à leur offre. Les tarifs démarrent souvent bas, à partir de quelques dizaines d'euros par mois. La tarification inclut souvent une part forfaitaire et une autre proportionnelle au volume. Les offres du marché s'adressent de la TPE à la grande entreprise. Parmi les premiers, on peut citer Xambox ou encore Arkansaas. Des archiveurs comme Everial ont ajouté l'électronique à leur offre d'archivage papier.

Les points à contrôler

Outre le prix, plusieurs aspects sont à vérifier avant d'externaliser. La labellisation du service d'archivage par des organismes comme la Fédération Nationale des Tiers de Confiance (www.fntc.org) ou l'adhésion du prestataire à la Fedisa garantissent un bon niveau de service. « *Il ne faut surtout pas se limiter à considérer la problématique de l'archivage électronique comme une simple dématérialisation des techniques traditionnelles d'archivage. ...Il faut, entre autres, apporter la preuve de leur intégrité tout au long de leur parcours, de la création à l'archivage, la donnée doit être récupérable facilement et efficacement, voire disponible en ligne* », souligne Jean-Marc Rietsch, président de la Fedisa. Très concrètement, l'accès en ligne aux documents archivés, le coût de cet accès, les formats de sauvegarde sont à contrôler. Notamment, la procédure de mise à disposition des informations en cas de rupture du contrat. Si tous ces points sont satisfaisants, l'externalisation est un moyen simple et accessible de mettre à l'abri ses documents sensibles. ■

Patrick BRÉBION

La facture électronique et le risque fiscal

PAR
Georges GRANGER
> Administrateur de l'AFAI (Association française des auditeurs et conseils informatiques)

La facture est le document de base pour la justification des opérations commerciales et de la comptabilité d'une entreprise, qu'il s'agisse des factures que l'entreprise émet à l'intention de ses clients, ou de celles qu'elle reçoit de ses fournisseurs. Les dispositions légales stipulent que les enregistrements comptables doivent préciser l'origine, le contenu et l'imputation de chaque donnée, ainsi que les références de la pièce justificative qui l'appuie.

La possibilité de trouver, à partir d'une écriture comptable, la pièce justificative qui étaie cet enregistrement et, inversement, de trouver à partir d'une pièce l'écriture comptable à laquelle cette pièce a donné lieu constitue le « chemin de révision » et est, tant en matière strictement comptable qu'en matière fiscale, une condition essentielle de régularité de la comptabilité. Lors d'un contrôle fiscal par exemple, une comptabilité peut être jugée non probante – et par conséquent entraîner une évaluation d'office – si elle ne permet pas de rapprocher les enregistrements comptables des pièces justificatives, et l'on sait par ailleurs que la facture d'achat mentionnant la TVA est une condition de forme de la déductibilité de cette dernière.

La facture fournit des informations détaillées sur le vendeur, l'acquéreur, la chose vendue et le prix, le régime de TVA applicable, et constitue ainsi un élément de preuve des opérations et un moyen de contrôle. C'est pourquoi elle fait l'objet d'une importante réglementation, la non-conformité des factures aux dispositions légales étant une infraction

sanctionnée de lourdes amendes pour l'émetteur.
Le volume considérable des factures émises ou reçues par les entreprises a amené, depuis un certain nombre d'années déjà, à envisager, comme pour d'autres opérations telles que les déclarations fiscales ou sociales, la suppression du document papier et son remplacement par des enregistrements électroniques. Toutefois, la conservation du caractère probant de ces documents nécessitait l'élaboration de règles permettant de garantir l'intangibilité des enregistrements (Articles 289-V et 289 bis du code général des impôts).

La facture électronique

Sous réserve du respect des conditions indiquées dans ces textes, une entreprise n'est plus tenue d'émettre des factures sur papier, la facture « immatérielle » étant alors reconnue comme un original.
Naturellement, l'internationalisation des affaires justifiait que des règles soient élaborées dans un cadre supranational et c'est pourquoi des directives européennes ont été élaborées dans ce domaine, en date du 20 décembre 2001 (2001/115/CE), la directive TVA (2006/112/CE) et celle du 13 juillet 2010 (directive 2010/45/CE), cette dernière devant être transposée en droit français à compter du 1er janvier 2013.
Il faut distinguer la facture « dématérialisée » c'est-à-dire une facture émise sur support traditionnel puis numérisée pour être archivée sous forme électronique, d'une facture émise dès l'origine en format numérique, qui constitue la facture électronique proprement dite. Dans le premier cas en effet, la version numérique n'est qu'une copie, alors que dans le second, la version électronique constitue un original.
Suivant les textes actuels, pour que la facture ait la valeur d'un original, il est nécessaire qu'elle soit transmise par un système d'échange de données informatisées tel que défini par la directive du 19 octobre 1994, ou au moyen d'une signature électronique conforme à la directive du 13 décembre 1999, afin que soient garanties l'authenticité de leur origine et l'intégrité de son contenu.
Le consentement du destinataire est nécessaire.
Le 13 juillet 2010, l'Union Européenne a adopté la directive 2010/45/CE. Suivant cette nouvelle réglementation européenne, qui doit donc être transposée en droit français pour application au 1er janvier 2013, c'est l'assujetti qui choisira la méthode qui lui conviendra le mieux pour garantir l'authenticité de l'origine et l'intégrité du contenu de la facture.
Le Code Général des Impôts (article 289-I-2) reconnaît la possibilité pour les fournisseurs de confier l'établissement matériel de leurs factures à un tiers, aux conditions suivantes :

- Le fournisseur doit donner mandat au tiers concerné pour émettre matériellement les factures en son nom et pour son compte.
- Le mandat doit prévoir que le fournisseur conserve la responsabilité de ses obligations en matière de facturation au regard de la TVA.
- Le contrat de mandat passé avec le tiers doit également obligatoirement contenir l'engagement du mandant de verser au Trésor la taxe mentionnée sur les factures établies en son nom et pour son compte, et conserver le double des factures ainsi que signaler toute modification dans les mentions concernant l'identification de son entreprise.

Les factures ainsi établies par le mandataire doivent comporter toutes les mentions prescrites par la réglementation. L'entreprise destinataire des factures doit vérifier l'authenticité et l'intégrité des factures reçues, c'est-à-dire la validité de la signature électronique, et s'assurer de l'authenticité et de la validité du certificat attaché à la signature électronique.

Obligations en cas de contrôle fiscal

L'administration peut, à tout moment, contrôler la signature électronique et s'assurer du respect des normes techniques définies. Si des manquements sont constatés par l'administration ou si les tests nécessaires à la vérification du système ne peuvent être effectués, le contribuable dispose d'un délai de 30 jours à compter de la date de réception du procès-verbal pour formuler des observations, apporter des justifications ou procéder à la régularisation du fonctionnement du système.
À défaut, il n'a plus la possibilité de télétransmettre ses factures. *Les factures transmises ne constituent plus alors des factures originales et la TVA mentionnée sur ces factures n'est pas déductible pour les clients. Le fournisseur doit alors émettre des factures papier ou des factures sécurisées au moyen d'une signature électronique pour permettre l'exercice du droit à déduction par ses clients.*
Les entreprises doivent assurer à l'administration un accès en ligne permettant le chargement et l'utilisation des données stockées, que le lieu de stockage soit en France ou hors de France.
L'assujetti doit s'assurer que le contenu des fichiers peut être restitué, sur demande de l'administration, en langage clair. Le système d'archivage doit permettre de répondre à des demandes sélectives de la part de l'administration. Si cette dernière le demande, la restitution des informations doit pouvoir être effectuée sur support papier.
En outre, si, durant le délai légal de conservation, l'environnement (matériel ou logiciel) est modifié, le contribuable doit assurer la conversion et la compatibilité des fichiers, sans altération des informations de base qu'ils contiennent, avec les outils existants au moment du contrôle. ■


© Kellis - Fotolia

Obligations de conservation et de restitution des factures

Pour les besoins fiscaux, les factures transmises par voie électronique doivent être conservées dans leur format original dans les conditions prévues par l'article L. 102 B du livre des Procédures Fiscales, sur support informatique pendant une durée au moins égale au délai du droit de reprise (l'année en cours et les trois années précédentes), puis sur tout support au choix de l'entreprise pendant les trois années suivantes. Notons toutefois que la prescription commerciale est plus longue et que les entreprises doivent conserver leurs factures pendant un délai de dix ans. Le lieu de stockage peut être en France ou dans un État étranger ayant passé une convention d'assistance mutuelle en matière fiscale. ■

Éric DUBOIS
Responsable de l'offre Clear' Invoice, Accelya

Accelya, opérateur historique de la dématérialisation des factures

Depuis plus de trente ans, Accelya opère sur le marché de la dématérialisation des transactions professionnelles, et en particulier des factures. Une expertise historique reconnue sur de nombreux secteurs d'activité, notamment sur le voyage d'affaires.

GPO Magazine : Pouvez-vous nous présenter Accelya ?

Eric Dubois : Accelya est un opérateur de dématérialisation des transactions professionnelles. Nous avons pour vocation d'aider nos clients à fluidifier les relations avec leurs partenaires commerciaux et à réduire leurs coûts, en leur proposant des services de traitement externalisés de transactions critiques, et ce, dans le respect de normes de qualité élevées. Factures, réservations de voyages, billets d'avions, instructions de paiements, transactions de cartes de crédit, sont autant de flux que nous traitons sur nos plates-formes. Ces traitements et transactions se font de manière complètement sécurisée et en parfaite conformité avec la législation en vigueur pour la dématérialisation puis pour l'archivage de ces documents.

GPO Magazine : Vous opérez sur des marchés particuliers ?

E. D. : Nous entendons être le partenaire de toutes les entreprises, quels que soient leur secteur d'activités ou la nature des documents et des transactions à traiter. Nous avons néanmoins une expertise très poussée dans certains secteurs comme le voyage. Depuis trente ans, nous sommes ainsi partenaire stratégique de IATA (l'Association Internationale du Transport Aérien). Nous opérons des services tels que le BSP (Billing and Settlement Plan) qui procure aux agences de voyages et compagnies aériennes du monde IATA fluidité, simplicité et transparence dans les transactions réalisées.

Par ailleurs, notre plate-forme de dématérialisation des factures Clear' Invoice est actuellement utilisée par plusieurs acteurs du voyage, tels qu'Avexia Voyages, Carlson Wagonlit Travel, Fram, Kuoni ou encore Amplitudes. Nous travaillons également avec les loueurs de voitures pour lesquels nous avons développé et opérons des plates-formes telles que Res@car (service de réservation en temps réel proposé par les loueurs de voitures à leurs clients professionnels) ou Edirent (plate-forme de dématérialisation des factures des loueurs de véhicules vers leurs clients business).

GPO Magazine: Où en est la réglementation en matière de dématérialisation fiscale des factures ?

E. D. : La réglementation a, cette dernière décennie, beaucoup évolué. Rappelons que la directive européenne de 2001 sur la dématérialisation fiscale des factures a été retranscrite en droit français en 2004. Elle autorise

Témoignage

Accelya partenaire d'Avexia Voyages pour la dématérialisation de ses factures

En 2011, Avexia Voyages, société spécialisé dans le voyage d'affaires et expert des PME, décide de s'appuyer sur Accelya pour la dématérialisation fiscale de près de 400 000 factures par an. « *Accelya a parfaitement compris nos besoins techniques pour l'intégration de la facturation électronique dans notre portail métier*, explique Julien Chambert, directeur du Contrôle de Gestion, Infrastructure et Systèmes au sein d'Avexia Voyages. *L'opérateur a également bien évalué nos besoins dans la relation client-fournisseur. Nous avons par ailleurs été séduits par l'ergonomie de la plate-forme Clear'Invoice, sa simplicité d'utilisation et sa fiabilité. Enfin, Accelya va nous permettre de développer notre Espace Client grâce à de nombreuses nouvelles fonctionnalités*». Quatre mois ont alors suffit pour la mise en œuvre de ce projet. « *Les clients bénéficient désormais d'un accès direct et facilité à leurs factures, tout cela depuis leur Espace Client personnel*, poursuit Julien Chambert. *Les services proposés sont plus nombreux, nos utilisateurs y gagnent en temps de traitement, sans compter qu'un client non dématérialisé actuellement, y trouvera un véritable gain économique : les frais de gestion liés à l'émission de factures électroniques par rapport au papier étant sensiblement réduits* ». Sur les 400 000 factures émises chaque année par Avexia Voyages, 216 000 sont actuellement dématérialisées fiscalement, et Avexia Voyages vient également de confier à Accelya la dématérialisation fiscale de ses factures fournisseurs. ■

Accelya en quelques chiffres

- **Chiffre d'affaires annuel :** 110 millions de dollars
- **Présence internationale** dans 10 pays sur tous les continents
- **Effectif :** plus de 2000 personnes
- Plus de **30 ans** d'expérience

l'échange de données informatisées structurées de type EDI ou la dématérialisation des factures dans des formats non structurés, de type PDF signé (fichier PDF contenant une signature électronique). La directive européenne a été révisée en 2006 puis en 2010. Cette dernière révision, qui devrait être retranscrite en droit local cet automne, autorisera très certainement une nouvelle possibilité (autre que le PDF signé ou l'EDI) pour faire de la dématérialisation fiscale des factures, et supprimer les factures papier. Etant au cœur de ces discussions, Accelya peut garantir à ses clients un service complet et juridiquement à jour.

GPO Magazine: Quels sont les enjeux de vos clients ?

E. D. : Aujourd'hui, la performance des entreprises est notamment liée à l'efficacité de leurs processus administratifs. Or, la facturation électronique rend l'ensemble du processus plus fiable, tout en ayant un effet positif sur sa rentabilité. Pour autant, les projets de dématérialisation fiscale des factures posent un véritable challenge aux entreprises en termes de déploiement. Si les partenaires commerciaux de nos clients font déjà de la dématérialisation, nous déploierons une solution très certainement en EDI. Si les contreparties de nos clients ne sont pas équipées, nous leurs proposerons des solutions de déploiement « clés en main », basées le plus souvent sur du PDF signé avec un portail de consultation et d'archivage légal des factures. Il leur suffit de donner leur accord pour ce nouveau service de facturation. À charge pour nous ensuite d'en assurer le traitement et le transport en vertu de la réglementation en vigueur. Nos solutions de déploiement sont ainsi suffisamment standardisées et paramétrables pour s'adapter à l'ensemble des problématiques de nos clients. ■

Pour en savoir plus

ACCELYA

ACCELYA France
3 boulevard des Bouvets
92741 NANTERRE CEDEX
Tél. : 01 47 29 76 11
E-mail : clear-invoice@accelya.com
www.accelya.fr