

L'intégrité un avantage concurrentiel pour les entreprises

(Easybourse.com) Face à tous les dangers qui la guettent, l'entreprise se doit de protéger l'ensemble de ses ressources, de ses valeurs et de ses hommes. Pour Michel Souque, président de Prim'x technologies, la sécurité des données est devenue impérative pour la survie de l'entreprise. Selon David Hornus, président de Risksgroup, la «sécurité économique», sous tous ses aspects, est l'huile qui permet le bon fonctionnement de la mécanique.

Selon Michel Souque, on estime que le périmètre de l'entreprise n'existe plus aujourd'hui : *«L'entreprise étant souvent internationale et se situant sur plusieurs lieux géographiques, il est difficile d'en faire le tour. Partant de là, certains experts estiment que d'ici 2010, tous les serveurs de données, même ceux hébergés intra-muros seront considérés comme étant dans un environnement hostile. Ce sera alors à la donnée de se défendre elle-même. Autrement dit, nous allons vers des organisations de données où le chiffrement sera généralisé ».*

Patrimoine informationnel, patrimoine éthique, patrimoine humain

Xavier Fauquet, expert de la société Devoteam Consulting estime que *«nous nous inscrivons aujourd'hui dans un monde de plus en plus ouvert où le système d'information de l'entreprise doit s'ouvrir afin de faciliter les échanges avec les clients, les partenaires, les fournisseurs de l'entreprise. L'enjeu en termes de sécurité est alors de permettre cette ouverture demandée par les métiers tout en fournissant un niveau de sécurité adéquat, protégeant les assets de l'entreprise.*

Par ailleurs, le développement fort des outils de mobilité permet un accès aux données de l'entreprise depuis différents types de terminaux : téléphones mobiles, PDA, poste de travail personnel via le télétravail etc... Le fait que l'accès à l'information ne soit plus cantonné aux murs de l'entreprise conduit à une dissémination de l'information sur ces différents terminaux. Ainsi, la défense périmétrique d'un système n'est plus suffisante : l'enjeu est alors de fournir les moyens adéquats afin de sécuriser l'information en tant que telle, où qu'elle soit, en interne ou en externe de l'entreprise et de contrôler qui peut y accéder avec le niveau de traçabilité associé.

Enfin, la multiplication des moyens d'accès à l'information entraîne une multiplication des possibilités et des formes d'attaques. Les attaques de type fishing se sont par exemple multipliées, notamment dans le domaine bancaire pour essayer de récupérer des informations confidentielles. Dans un autre registre, le spamming qui représente pratiquement 80 % du trafic e-mail doit aussi être traité par les entreprises afin de préserver l'efficacité des moyens informatiques mis à disposition des collaborateurs».

Enfin, David Hornus rappelle que *«les nouveaux entrants dans la mondialisation cherchent à acquérir nos connaissances pour satisfaire nos «normes» et nos exigences. Pour eux, gagner du temps est primordial. Il faut alors faire attention aux écoutes téléphoniques, aux vols de documents confidentiels, etc».*

Au-delà du patrimoine informationnel, l'entreprise doit également protéger son patrimoine éthique (corruption, blanchiment, fraude). Or la désinformation, la manipulation de l'information, l'influence ou la censure sont des pratiques en forte croissance. Elles peuvent influencer un cours de bourse, masquer une OPA, ternir la réputation d'un produit ou d'une firme jusqu'à provoquer des boycott, etc.

Selon Philippe Montigny, président de l'agence Ethic-Intelligence, *«une personne de l'entreprise peut mettre en danger le patrimoine éthique de celle-ci en commettant un acte illégal aux yeux de la loi ou répréhensible au regard de l'opinion publique parce qu'il serait considéré comme illicite. Par ailleurs, un concurrent peut attaquer l'image de l'entreprise en l'accusant faussement d'un acte illégal ou illicite».*

Les péripéties sont nombreuses, mais les entreprises ne communiquent que très peu, voire jamais sur ces aspects de leurs activités. En avril dernier, le groupe parapétrolier Baker Hughes s'est vu contraint de passer un accord avec le Ministère de la Justice (Department of Justice) et la Securities and Exchange Commission (SEC). D'une sévérité sans précédent dans le cadre du FCPA, l'accord prévoyait le paiement d'une amende de 44,1 millions de dollars d'amendes civiles et pénales et le remboursement des profits tirés de l'opération en cause.

L'exemple tiré de l'affaire ABB est plus parlant. Suite à la découverte en interne du versement de commissions occultes à un fonctionnaire nigérian, la société avait alerté le Ministère de la Justice. En dépit du plaidé coupable, ABB a été condamnée au pénal à payer une amende de 10,5 millions de dollars.

Par la suite, la SEC a obtenu une peine d'amende de 5,9 millions de dollars au civil. Pour le suivi de cette affaire, les avocats d'ABB lui ont facturé 43 000 heures de travail, au tarif horaire de 400 dollars. Il ne s'agissait pas des seules peines infligées, puisque la SEC a mandaté une société indépendante pour assurer un monitoring d'ABB.

Enfin, comme les preuves de la corruption avaient été mises à jour au cours d'un audit conduit dans le cadre de la cession d'une filiale, la SEC a contraint ABB à réaliser un audit mondial de toutes ces opérations, sur les six années antérieures. Ceci a ainsi retardé la cession de la filiale de plus d'un an. (Elements repris du Kroll Global Fraud Report de Juin 2007 sur la corruption et la loi sur les pratiques de corruption à l'étranger (*Foreign Corrupt Practices Act*)).

Mais pour David Hornus, président de Risksgroup, «*la menace la plus létale est sans conteste la perte humaine. Enlèvements et demandes de rançons se multiplient et pour les anticiper ou les réduire au maximum, il faut bien avoir une démarche d'Intelligence sécuritaire ... Aujourd'hui d'un point de vue sécuritaire, les seuls vrais problèmes dont on entend parler concernent les enlèvements d'occidentaux au Nigeria*».

Des enjeux importants

Selon Alain Juillet, «*la violation d'un secret d'entreprise au niveau d'un savoir faire, d'un projet de produit, d'une divulgation de contrat, pour quelque motif que ce soit peut avoir des conséquences dramatiques pour l'entreprise et sur l'emploi. C'est ainsi que la connaissance détaillée des bilans et comptes d'exploitation par un concurrent peut lui permettre de prendre le contrôle de l'entreprise dans des conditions très avantageuses. Chaque société, chaque pays a des secrets qu'il doit garder pour préserver l'avenir de ses salariés et de nos enfants. C'est particulièrement vrai pour les technologies clés et les entreprises sensibles*».

Nouvelle attaque américaine contre l'A 380
Le super-jumbo d'Airbus pourrait être dangereux pour les autres avions, en raison des turbulences qu'il crée dans son sillage.

Airbus Boeing (Le figaro du 6 octobre 2005)

Nouvelle attaque frontale des Américains contre l'A 380

Conséquences :
387 millions de \$ pour Airbus contre 14 milliards de commandes pour Boeing

De même, l'atteinte au patrimoine informationnel d'une entreprise peut l'amener à perdre d'un avantage compétitif dans le domaine de la recherche-développement. On se souviendra de l'affaire retentissante concernant l'industriel français Valeo il y a deux ans. Celui-ci avait été espionné par une stagiaire chinoise qui avait détourné des fichiers contenant des informations sensibles pour l'entreprise. À l'époque, cet incident avait amené le président de la société à communiquer pour rassurer ses actionnaires.

La défaillance d'une entreprise au niveau de sa sécurité peut par ailleurs porter atteinte à l'image de l'entreprise, avec des risques importants d'effondrement du cours de bourse. C'est ainsi qu'en 2005, rappelle Philippe Montigny, «*l'entreprise de télécommunications américaine Titan Corporation, un des fournisseurs du ministère américain de la défense qui devait être racheté par Lockheed s'est vue condamnée à une amende de 28,5 millions de dollars pour avoir versé un pot de vin de 2 millions de dollars payés pendant la campagne présidentielle au Bénin. Le cours de bourse de la société s'est effondré de 46%. 800 millions de dollars se sont évanouis en quelques séances*».

Nicolas Moinet précise que «*dans nos sociétés du spectacle, il est de plus en plus courant de perturber la boucle adverse par des attaques informationnelles. Les marchés et les actionnaires aiment le politiquement correct et veulent impérativement des pratiques éthiques, même si la réalité est parfois bien différente. Ils détestent donc la mauvaise réputation et les rumeurs dérangeantes*».

Le disfonctionnement ou l'inaction dans le domaine de la sécurité peut conduire l'entreprise à être condamnée à verser des indemnités/ dommages-intérêts. Suite à la jurisprudence issue de l'attentat de Karâchi, une l'entreprise peut être jugée responsable de ne pas avoir suffisamment informé ses salariés du degré de danger et de ne pas les avoir fait suffisamment accompagner.

C'est ainsi également qu'en l'absence de garantie suffisante, une entreprise peut être accusée de fraude du seul fait de l'acte malveillant d'un de ses employés et devoir payer des millions de dollars ou d'euros d'amende. Dans certains pays «ne pas savoir» ne constitue pas un argument de défense. *«Est considéré comme illégal le versement d'une commission à un tiers lorsque le donneur d'ordre a connaissance que tout ou partie de la somme sera remise directement ou indirectement à un représentant officiel d'un pays étranger. Il en va de même si le donneur d'ordre ne tient pas compte ou ignore de manière délibérée cette information»*, précise le Department of justice des Etats Unis.

Selon Michel Souque, *«des sociétés bancaires ont été condamnées pour avoir perdu des fichiers clients qui contenaient des informations confidentielles, notamment des renseignements sur l'état de santé obtenus dans le cadre de souscription de prêts. Des class actions ont pu être intentées et des indemnités plus que conséquentes ont dû être versées»*.

Comment agir ?

Tout d'abord en formant et en informant. Selon David Hornus, *«former, informer les salariés, expatriés et familles est désormais un impératif»*. Il ajoute qu' *«il vaut mieux verser quelques milliers d'euros pour former, informer, accompagner, plutôt que de se dire que ça n'arrive qu'aux autres et que le jour où il y a un problème, l'enlèvement, l'assassinat ou la mort d'un de vos expatriés dans le cadre d'un attentat, vous fassiez l'objet d'un procès de la part de la famille et que vous perdiez non seulement plusieurs millions d'euros mais également votre image de marque, votre réputation, et au final des parts de marché. Les américains disent il vaut mieux un bon arrangement qu'un mauvais procès ! On pourrait aussi dire «il vaut mieux prévenir que guérir»*.

Par ailleurs, l'entreprise peut se protéger en mettant en place des dispositifs efficaces. Les dispositifs «périmétrique» (firewall) et les mécanismes logiques de gestion de droits d'accès aux données constituent des barrières indispensables pour la protection des données.

Mais selon Michel Souque, le chiffrement constitue la protection absolue. C'est un processus mathématique qui transforme les données les rendant lisibles uniquement par le biais d'un secret, généralement propre à l'utilisateur.

D'autre part, la certification Ethic Intelligence peut constituer un moyen efficace pour prévenir les attaques contre le patrimoine éthique de l'entreprise.

«Cette certification ressemble à une sorte de contrôle technique automobile. Nous allons vérifier dans l'entreprise que les éléments nécessaires au contrôle du point de vue éthique sur les questions de l'anti-blanchiment et de l'anti-corruption ont bien été mis en place», indique Philippe Montigny, le président de la société.

«Dès lors, s'il y a une véritable accusation de corruption ou de blanchiment, la certification permet de mettre en évidence que le management de l'entreprise avait fait tout ce qu'il fallait pour prévenir ce délit. L'acte de malveillance a donc été commis par un employé de l'entreprise à l'encontre des règles édictées par cette dernière. Enfin, lorsqu'une entreprise concurrente porte une allégation à l'encontre d'une autre entreprise, la certification délivrée permet d'inverser la charge de la preuve. C'est donc à l'entreprise accusatrice d'apporter l'attestation de ses dires», ajoute l'expert.

Ainsi, même s'il ne s'agit pas d'une défense absolue, démontrer que toutes les transactions avec des tiers ont fait l'objet d'un audit minutieux peut infléchir de manière significative la «présomption de connaissance».

Dans le cas d'ABB, le versement de commissions occultes n'était pas seul en cause : la SEC a noté que les contrôles internes qui auraient permis de détecter et d'empêcher toute infraction au FCPA étaient insuffisants.

Imen Hazgui