Qualification et quantification des risques en vue de leur transfert : la notion de patrimoine informationnel.

Jean-Laurent Santoni

Marsh Risk Consulting France

1 Introduction

Pour les systèmes d'information, un des points majeurs en matière de gestion des risques et de leur transfert tient dans la qualification des objets informationnels et de l'identification des flux échangés entre les différents acteurs (qualification juridique et technique, et qualification des évènements redoutés) d'une part, et d'autre part dans la quantification des enjeux, qu'il s'agisse des pertes supportées, des frais de continuité engagés ou des dettes de responsabilités en découlant.

Qualification et quantification supposent alors de quitter la sphère technique et de se placer dans une double perspective : l'économie des immatériels, d'une part, et l'écologie des immatériels, d'autre part.

L'économie des immatériels est fondée sur l'émergence de la notion de patrimoine informationnel. Le patrimoine informationnel devra être appréhendé d'une part en ce qu'il peut être en tant qu'actif patrimonial l'objet du risque, la cible du préjudice, et d'autre part en ce qu'il peut être le fait générateur du risque, la source du préjudice, élément de passif patrimonial. Une réflexion devra être menée sur les composantes du patrimoine informationnel, essentiellement sur les données (logiciel, base de données, informations) et les traitements (flux et échanges). Cette réflexion devra intégrer des aspects juridiques stricto sensu (qualifications et régimes juridiques), mais également des aspects économiques (analyse de la valeur) si l'on veut appréhender les deux éléments clés du risque que sont la définition des faits générateurs et la quantification des pertes induites.

L'écologie des immatériels sera, elle, fondée sur l'émergence des nouveaux rapports entre l'homme et l'environnement informationnel mondial, dans une perspective où se mêleront la morale et le droit. L'expression d'écologie renvoie à une approche internationale et à la mise en œuvre de politique d'incitation et de répression des comportements.

2 Qualification et quantification des risques en vue de leur transfert : la notion de patrimoine informationnel

La révolution technologique, qui bouleverse les modes opératoires et modifie la façon dont la valeur est créée a engendré une nouvelle économie composée d'acteurs prestataires de services immatériels. Outre l'émergence de cette nouvelle

économie numérique, nous assistons à un déplacement de la valeur, du matériel vers l'immatériel. Ainsi, pour l'entreprise au sens large, on parlera de plus en plus de concepts tels que le « patrimoine informationnel », démontrant par là la reconnaissance du poids grandissant de la valeur des informations par rapport à leur support ou, plus généralement, aux seuls actifs physiques. Les composantes du patrimoine informationnel sont essentiellement les données (logiciel, base de données, informations) et les traitements (flux et échanges).

2.1 L'environnement numérique : immatériel et sans frontières

L'environnement numérique se caractérise par les principales spécificités suivantes :

Un environnement ouvert Les réseaux numériques sont totalement ouverts par conception, accessibles à tous ceux qui sont connectés. Le nombre d'utilisateurs est *a priori* illimité. En conséquence, le système d'information d'une entreprise connectée au réseau numérique est relié à l'extérieur.

Une dématérialisation des échanges et des biens Un commerce sans échange physique entre acheteur et vendeur (commerce électronique),

Un réseau qui n'appartient à personne en tant que tel Seule l'extrémité, *i.e.* la tête du réseau, appartient à une entreprise ; c'est également un univers sans autorité centrale, ni juridiction au niveau international.

Dans ce contexte, on comprendra que les aspects liés à la sécurité, à l'authenticité et à la confidentialité de l'information seront de plus importants que dans un environnement fermé, à l'image d'un environnement physique. On retiendra également la dépendance croissante des entreprises envers ce type de technologies (qui peut aujourd'hui se passer des biens incorporels ?) car elles procurent un accès au consommateur, particulier ou entreprise, et permettent une diminution des coûts. *A contrario*, la défaillance de tout ou partie de cet ensemble peut entraîner des pertes graves pour l'entreprise.

Quelle est la nature des risques pesant sur l'environnement numérique et les biens incorporels ?

Les caractéristiques de l'environnement numérique se traduisent par un risque d'amplification ou de contagion par un effet de domino. En considérant les risques en termes de fréquence et de gravité, il est possible de mettre en évidence au moins quatre domaines où les technologies numériques et les biens incorporels amplifient l'exposition aux risques :

1. L'augmentation du nombre potentiel des réclamations : le nombre d'acteurs et de connectés augmente de manière exponentielle.
2. L'augmentation de la gravité potentielle des sinistres :

- l'offre est de plus en plus riche et davantage mise en valeur ;
- afin d'augmenter le flux de leurs revenus à l'international, les entreprises utilisent de plus en plus les technologies numériques comme outil de communication et d'échange.

3. La multiplication des mises en cause potentielles : on assiste à une démultiplication du nombre d'intervenants ayant une implication directe ou indirecte dans les technologies numériques.
4. L'augmentation de la complexité des risques traditionnels et des procédures juridiques : le caractère international d'Internet et du commerce électronique, implique un risque accru de conflit de loi. Une fois l'information ou l'offre émise sur le réseau, sa diffusion peut échapper totalement au contrôle de son auteur. De fait, il paraît impossible de respecter l'intégralité des législations nationales de par le monde.

En conclusion, si les activités liées aux technologies numériques ont fait apparaître de nouveaux types de risques, dans un grand nombre de cas, ce sont des risques classiques qui se trouvent démultipliés et amplifiés par le recours à ce nouveau support.

2.2 Un déplacement du risque : de l'atteinte physique à l'atteinte logique et incorporelle

Parallèlement à la migration de la valeur vers l'immatériel, on assiste depuis une vingtaine d'années à une modification de l'environnement hostile qui concerne les sources de pertes occasionnées aux entreprises. La malveillance, qu'elle soit inspirée par des motifs mercantiles ou des intentions purement malignes, continue de croître pour prendre des formes de plus en plus inquiétantes, comme en témoigne l'actualité la plus récente. Sans nécessairement faire preuve de sensationnalisme, nous assistons à une escalade dans les attaques logiques contre les systèmes d'information des entreprises ou des administrations, avec le franchissement d'une nouvelle étape : le réseau lui-même devient la cible, avec un objectif de paralysie à l'échelle mondiale !

Cependant, tous les acteurs économiques ne sont pas logés à la même enseigne dans l'échelle des risques encourus. En conséquence, gérer le risque lié à l'environnement numérique et pesant sur les biens incorporels implique une analyse spécifique à chaque utilisateur.

2.3 Les types d'activités à risques

Les expositions aux risques varient en fonction de chaque type d'activités. Néanmoins, il est possible de mettre en évidence un certain nombre de facteurs de risques et corrélativement des impacts spécifiques, comme le montrent les exemples suivants :

1. Dépendance à une technologie complexe qui peut être fragile et insuffisamment testée pour sa tolérance aux défauts : dans ce domaine où l'innovation

produit et la communication marketing sont essentielles, il faut aller vite et « sortir » le premier.

2. Concentration d'activités et de services auparavant éclatés, voire externalisés : publicité, paiement, livraison...
3. Nécessité technique de connecter des systèmes internes critiques au monde extérieur :
   - contrôle des commandes et des inventaires ;
   - comptabilité et paiement ;
   - système de contrôle d'accès ;
   - système d'identification et d'authentification.
4. Risque accru de fraude technologique ; défis de *hacking* ciblant des entreprises connues ou fortement protégées.
5. Extension de la législation du droit d'auteur aux logiciels, au contenu et aux applications commerciales ; fréquence accrue des litiges fondés sur le droit d'auteur, nature complexe de ces droits dans le monde.

2.4 Les risques immatériels susceptibles d'être couverts par un contrat d'assurance

Fraude informatique Enlèvement fautif de biens matériels (argent, titres boursiers et autres biens) et immatériels (services, propriété intellectuelle et données) effectué par les salariés ou les non-salariés.

Vol de données électroniques et d'actifs électroniques Enlèvement fautif du code logiciel, des informations sur les fournisseurs, des informations confidentielles ou propriétaires, dont la propriété intellectuelle, le code source, les données clients, les informations électroniques du fait d'un accès non autorisé ou d'une utilisation non autorisée des réseaux informatiques.

Vol des ressources du système d'information Les ressources informatiques ou télécoms sont utilisées à des fins non officielles et non autorisées.

Divulgation d'actifs électroniques Divulgation non autorisée d'informations propriétaires ou confidentielles enregistrées sous format électronique, résultant d'un délit informatique, d'un acte malveillant (attaque), ou d'une erreur non intentionnelle de la part du personnel informatique autorisé dans l'exercice normal de ses fonctions.

Actes malveillants (attaques) Modification ou dégâts causés aux systèmes ou aux données dans le but de nuire, de saboter, d'agir de façon malveillante, de se venger, par motivation politique ou sociale, pour faire une farce ou s'amuser.

Endommagement des informations électroniques À cause d'une erreur humaine ou du fait d'un acte ou d'une erreur non intentionnels de la part du personnel informatique autorisé dans l'exercice normal de ses fonctions.

Code nuisible Implantation, introduction, et diffusion de virus informatiques, de bombes logiques, de chevaux de Troie et d'autres formes de code malveillant.

Déni de service Une attaque cause la dégradation des performances ou la perte du service (interruption de service ou arrêt) d'un site Web ou d'une application réseau.

Perte de service Arrêt du système informatique, « crash », dégradation des performances du fait d'une erreur non intentionnelle de la part du personnel informatique autorisé dans l'exercice normal de ses fonctions.

Interruption du service hors site Dangers physiques (tels que les ouragans et les incendies), les attaques, les accidents, et le dysfonctionnement de l'infrastructure de communication du réseau, dont les satellites, les lignes téléphoniques, les câbles, les lignes électriques et les câbles optiques.

Risques liés au e-commerce Authentification (validité d'une transmission, du message ou de l'expéditeur), non-répudiation (service cryptographique qui empêche légalement l'expéditeur d'un message ou l'acheteur de nier être l'auteur du message ou de nier la transaction à une date ultérieure).

Courrier électronique d'entreprise Le type d'informations et le contenu des courriers électroniques peuvent être interceptés par des personnes non autorisées lors de litiges avec des tiers et des salariés. Les défaillances de la sécurité (par ex. : mots de passe et cryptage) peuvent amener à la divulgation d'informations propriétaires (espionnage industriel possible) ou en une situation embarrassante.

2.5 L'assurance du patrimoine informationnel

Aujourd'hui, les échanges économiques se dématérialisent et passent du monde réel au monde virtuel. De simple outil, le système d'information se place au cœur de l'entreprise et constitue un élément essentiel de sa compétitivité, interconnecté avec des réseaux externes. Système nerveux et mémoire de l'entreprise, élément souvent crucial de sa compétitivité, il fait l'objet de mesures de sécurité préventives. Les estimations réalisées montrent que le budget affecté à la prévention constitue de 10 à 20 % du budget informatique, lequel souvent représente de 1 à 2 % du chiffre d'affaires.

Au-delà d'un certain niveau, les investissements supplémentaires dans la prévention perdent de leur efficacité. En outre, celle-ci ne parviendra jamais

à prendre en compte l'ensemble des aléas, dont le facteur humain. Se pose alors la question du choix entre prévention et assurance dans le cadre d'une approche globale de la sécurité et du budget qui lui est consacré.

Les couvertures d'assurances doivent donc intégrer le « capital information » indispensable à l'activité des entreprises :

1. les données nécessaires à la transaction commerciale ;
2. le patrimoine constitué par le système d'information.

Pourtant, les réponses des assureurs en matière de couvertures immatérielles sont longtemps restées morcelées, les garanties proposées étant soit des extensions dans le cadre de contrats « Tous Risques Informatiques » excluant systématiquement les risques logiques, soit des extensions « Sabotage Informatique » à partir de protections « Fraude » excluant alors toute autre forme de malveillance. Enfin, le montant des garanties accordées ne reposait pas sur une valorisation préalable de la matière assurée et se révélait la plupart du temps très insuffisant.

Ces dommages sont aujourd'hui assurables à partir des polices d'assurance dédiées, proposant des capacités croissantes. Ce nouveau concept d'assurance accorde aux entreprises une protection financière efficace contre l'ensemble des vulnérabilités internes ou d'origine externe, pouvant affecter l'intégrité et la disponibilité de leur système d'information.

2.6 Le cadre général des polices dédiées

Généralement de type « Tous Risques Sauf », il couvre :

1. les frais supplémentaires d'exploitation informatique, permettant notamment de financer un plan de secours ;
2. les frais supplémentaires additionnels ;
3. les pertes d'exploitation ;
4. avec, notamment, la prise en charge des frais engagés pour reconstituer les programmes et données informatiques, même en l'absence de sauvegardes exploitables.

Cette garantie peut être mise en jeu lorsque l'information a été détruite, altérée, volée ou perdue, et ce quels que soient :

1. le type de sinistre (incendie, dégât des eaux, sabotage, virus, intrusion par les réseaux ouverts tels qu'Internet, carence de réseaux externes...) ;
2. la nature de l'information (progiciels, développements spécifiques, CAO-DAO, bases de données, paramétrages...) ;
3. le média utilisé (disques, bandes...).

Sont considérées par les compagnies d'assurance comme dommages immatériels informatiques les atteintes à la disponibilité et à l'intégrité d'un système d'information pouvant entraîner des pertes pécuniaires :

1. qu'il y ait ou non atteinte à l'intégrité physique de l'outil informatique ou d'un support d'informations ;
2. que les événements dommageables résultent d'une erreur de manipulation ou de pupitrage des supports de données ou d'un acte de malveillance.

Il s'agit de couvrir :

1. les frais de reconstitution des informations détruites ou altérées ;
2. les frais supplémentaires d'exploitation informatique ;
3. les pertes d'exploitation ou de marge brute d'exploitation ;
4. les pertes indirectes (intérêts débiteurs, intérêts créditeurs, pénalités contractuelles) ;
5. les frais de recherche, d'expertise, de décontamination des données infectées ;
6. les pertes de valeurs suite à fraude ;
7. les pertes d'image ;
8. la gestion de crise.

2.7 Cas particulier de l'assurance des entreprises clientes : notion de « Dommages Pour Compte »

Une évolution récente du concept d'assurance du patrimoine informationnel a permis d'envisager la couverture des entreprises utilisatrices de produits et services diffusés par la société assurée sur des bases contractuelles dites de « Dommages Pour Compte », le prestataire ayant transféré à l'assurance pour financement les risques encourus par ses clients dans le cadre d'une rupture de services en dehors de toute nécessité immédiate de recherche en responsabilité du prestataire à l'origine des préjudices subis dans des délais rapides en combinaison, le cas échéant, avec des couvertures Responsabilité Civile pour augmenter la capacité indemnitaire en cas de faute avérée.

L'objectif recherché n'est pas tant la sécurisation du client final en lui garantissant la bonne fin de l'opération réalisée ou de la prestation délivrée que la préservation de l'image de marque de la société prestataire.

A partir d'une couverture d'assurance dédiée à la relation contractuelle prestataire/client, le prestataire peut articuler et, éventuellement, étendre sa limitation contractuelle d'indemnité en proposant, dans le cadre de son contrat commercial, le financement :

1. de solutions palliatives matérielles et informationnelles dans l'hypothèse où la technologie informatique ou le service associé est détruit ou indisponible ;
2. des pertes d'activités consécutives au préjudice subi, tant en frais supplémentaires qu'en pertes d'exploitation.

Ces différents types de risques, bien qu'ayant des faibles probabilités d'occurrence en raison de la qualité des technologies déployées et des sécurités organisationnelles mises en place, peuvent générer une crise majeure car la confiance dans l'ensemble de la chaîne technologique sera remise en cause par les utilisateurs.

La réponse à de tels cas ne peut résider uniquement dans un transfert financier du risque vers des tiers, en raison, d'une part, de l'impact sur l'image et la marque, et, d'autre part, parce que la survie de l'entreprise dépend moins de sa capacité à indemniser des tiers que de son aptitude à réagir efficacement à cette crise.