Assurances

Assurances

Les risques informatiques et l'assurance

Rémi Moreau

Volume 61, numéro 4, 1994

URI : https://id.erudit.org/iderudit/1104981ar
DOI : https://doi.org/10.7202/1104981ar

Aller au sommaire du numéro

Éditeur(s)

HEC Montréal

ISSN

0004-6027 (imprimé)
2817-3465 (numérique)

Découvrir la revue

Citer ce document

Moreau, R. (1994). Les risques informatiques et l'assurance. *Assurances*, *61*(4), 697–703. https://doi.org/10.7202/1104981ar

Garanties particulières

par

Rémi Moreau

Les risques informatiques et l'assurance

Nous désirons résumer ici une étude faite sur les risques informatiques, laquelle fut publiée dans le supplément « Les Cahiers pratiques » du 11 décembre 1992 de *L'Argus*. Nous ferons le point sur les garanties d'assurance offertes sur la sinistralité et la prévention de ces risques. Nous reprendrons également certaines idées émises dans une autre étude, celle-ci publiée dans *L'Argus* du 30 août 1993[1].

L'évolution

L'évolution des risques informatiques assurables est considérable, suivant, en cela, l'évolution de l'ordinateur. D'une « mécanique impressionnante par son volume, curieuse par son côté hétérogène et bruyante à cause des moteurs des trieuses des cartes perforées » des années 1950, nous nous retrouvons aujourd'hui, en l'espace de quelques décennies, avec un instrument technologique extrêmement sophistiqué, réduit, rapide, convivial et performant.

Il n'est pas étonnant de constater que les ordinateurs de la première génération, constitués par des composantes électriques et électromécaniques, étaient assurés par les polices *bris de machines*.

Rapidement, le besoin est apparu d'innover par des formulaires particuliers et d'assurer non seulement le bien informatique et le matériel d'environnement mais encore les frais de restauration des informations enregistrées sur les supports d'information détruits ou détériorés à la suite d'un dommage

[1] Le Cahier pratique intitulé « Les risques informatiques » est rédigé par M. Daniel Lasserre. La deuxième étude, intitulée « Le chiffre noir », est signée par Gérard Defrance.

matériel et la reconstitution des fichiers informatiques : il s'agit de l'assurance des médias ou des supports d'information. Pour compléter l'éventail des garanties des années 1970, les souscripteurs proposèrent la garantie des frais supplémentaires d'exploitation.

Où en sommes-nous, à l'aube de l'an 2000, dominés par les microprocesseurs, les modem internes, les lecteurs optiques et les imprimantes laser, en terme de garanties d'assurance, après la féconde période d'évolution technologique des dix dernières années que nous venons de traverser ?

Les principales garanties

Voici le panorama des principales garanties actuellement disponibles non seulement sur le marché français, d'où émanent nos sources, mais encore sur le marché nord-américain :

1. Les dommages matériels

Sont couverts les frais découlant de la disparition, de la destruction ou de la détérioration des biens informatiques et du matériel d'environnement à la suite d'un incendie, d'une explosion, d'un acte de malveillance, d'un acte négligent commis par un préposé ou un tiers, d'un accident d'origine externe causé par un phénomène électrique, d'un vol ou d'une tentative de vol sur les lieux. La perte ou l'endommagement des biens en cours de transport qui résulte d'un incendie, d'une explosion, de la collision ou du vol du véhicule est également couverte.

2. Les frais de reconstitution des informations

Sont couverts les frais de restauration et de reconstitution des informations enregistrées sur les supports d'information détruits ou détériorés suite à un dommage matériel garanti, ainsi que les frais d'étude, d'analyse et de programmation engagés exclusivement pour adapter le logiciel d'application à un nouveau matériel informatique de rendement

équivalent, lorsque le matériel de traitement de l'information n'est plus réparable ou disponible.

3. Les frais supplémentaires d'exploitation

Sont couverts les frais ci-après énumérés, engagés dans le but de poursuivre des opérations courantes de traitement de l'information interrompues à la suite d'un sinistre matériel garanti : les frais de location de matériel, de services de remplacement provisoire et les frais supplémentaires de main-d'oeuvre et de transport.

4. Les intérêts de découverts bancaires

Sont couverts les remboursements des intérêts de découverts bancaires réglés par l'assuré suite à l'impossibilité d'effectuer des opérations de facturation et de relance de facturation déjà réalisée et résultant d'un dommage matériel aux biens informatiques.

5. Le sabotage immatériel

Son couverts les frais ci-après énumérés qui résultent d'une infection informatique (virus) ou d'un sabotage manuel, suivant un acte de malveillance, atteignant les biens informatiques ou le matériel d'environnement : les coûts, honoraires et frais engagés pour établir l'acte délictueux, les frais de décontamination des données et des programmes, les frais de reconstitution des informations s'il existe des sauvegardes immédiatement accessibles et qui sont à jour et les frais occasionnés par la perte de fonds ou de biens mémorisés ou emmagasinés appartenant à l'assuré ou confiés par des tiers et résultant d'un détournement, d'une fraude, d'une escroquerie, d'un vol, d'un acte de malveillance ou de sabotage.

6. Les pertes d'exploitation après un dommage matériel

L'assureur indemnise l'assuré de la perte de marge brute de l'entreprise et des frais supplémentaires d'exploitation destinés à réduire la perte de chiffres d'affaires, qui résultent

d'un dommage matériel garanti ou d'un vol ou d'une tentative de vol.

7. Les pertes d'exploitation après une interruption de service

L'assureur indemnise l'assuré de la perte et des dommages identifiés précédemment causés par une interruption de service d'origine externe des biens ou du matériel informatiques, pourvu que telle interruption soit consécutive à des coupures ou à des dysfonctionnements dans l'alimentation ou qui surviennent à la suite d'une interruption de service des biens assurés résultant d'une panne du système informatique. Il est entendu que cette garantie ne s'applique que si les coupures, les dysfonctionnements ou les pannes dues à un acte accidentel ou à un acte malveillant ou encore que s'ils sont liés à un phénomène naturel.

Les conseils du courtier sont très précieux, non seulement pour adapter l'une ou l'autre garantie aux risques susceptibles de se matérialiser, mais en vue de coordonner, sous un même programme d'assurance, global, cohérent et articulé, les différentes garanties directes et indirectes, accidentelles ou criminelles, principales et accessoires. En outre, les garanties doivent être exprimées sur la base d'une indemnité de remplacement (ou valeur à neuf), durant au moins les deux premières années à compter de la mise en service des biens informatiques assurés. La tarification prend en compte la valeur assurable, d'une part, mais aussi la mise en place d'un service d'entretien, d'autre part.

L'assureur ne couvre pas les frais ou les dommages couverts en vertu d'un contrat de maintenance, ceux qui sont dus à des modifications non conformes aux fiches techniques du constructeur, ceux qui sont dus à la détérioration normale ou progressive, ou ceux qui font l'objet d'une autre assurance complémentaire.

La sinistralité

Les causes des sinistres informatiques se classent dans trois catégories principales : ceux liés à des actes malveillants, ceux liés à des actes accidentels et ceux liés à des erreurs. Selon les statistiques, les malveillances (vols de matériels, fraudes, attaques logiques) représentent 57 % des sinistres informatiques déclarés. Si on additionne les sinistres accidentels de même que les erreurs de saisies ou de programmations, on arrive à un plafond de 70 %.

On peut encore identifier les sinistres informatiques selon les types de dommages. Les voici, par ordre d'importance : l'incendie, les dommages par l'eau, les sinistres criminels (le vol, la destruction volontaire, le détournement et la fraude), les catastrophes naturelles (la foudre) et les dommages électriques.

À titre d'exemples de dommages matériels, mentionnons : un incendie d'un centre informatique d'une banque ; une médiathèque enfumée à la suite d'un incendie, sans que les données n'aient été sauvegardées ; un « concentrateur » de télécommunications d'un réseau de vente par correspondance est brûlé, d'où une perte d'exploitation engendrée par l'interruption des commandes avant que le raccordement à un réseau de secours ne soit opérationnel ; une inondation est provoquée par une rupture de canalisation ; une explosion due à la foudre propagée sur une liaison de télécommunication détruit un micro-ordinateur servant à analyser un système d'imagerie médicale.

Selon les statistiques françaises, les malveillances (vols de matériels, fraudes, attaques logiques) représentent 57 % des sinistres informatiques déclarés. Si l'on tient compte des accidents, des erreurs de saisies ou de programmations et des malveillances, on arrive à 70 %.

Voici quelques exemples de risques criminels qui se sont avérés très dommageables :

- le détournement de fonds : par la modification illicite d'un programme de versement d'allocations

d'indemnités, le fraudeur, communément appelé le « voleur en blanc », peut réussir à effectuer des virements de fonds, faibles, mais continus ; ce type de fraudes peut durer plusieurs années avant d'être découvert ;

- le détournement de biens : l'intrusion d'un « pirate » permet de centraliser les disponibilités de points d'approvisionnements d'une coopérative laitière, de modifier la table de composition en matières grasses, ce qui aboutit au prélèvement d'excédent pendant près d'un an ;

- le sabotage industriel : (1) le programme robotisé d'une entreprise est infecté sous prétexte d'une fausse maintenance, ce qui a pour effet de faire vibrer le bras de manipulation, qui subit des dommages matériels très importants ; (2) suivant une menace de chantage au virus dans une institution financière, les responsables entreprennent de vérifier le système et ils changent les mots de passe par mesure de sécurité ; c'est à ce moment que les pirates, à l'écoute du réseau, détectent les mots de passe et introduisent un virus actif dans le système ; suivant une demande de rançon refusée, le virus est déclenché ;

- la fuite d'informations : le fraudeur réussit à copier un fichier bancaire reliée à la décision de consentir des crédits aux entreprises, ce qui lui vaut de recenser celles qui sont en difficultés ; il menace alors ces entreprises de divulguer cette information confidentielle aux fournisseurs et aux clients contre des rançons alléchantes.

La prévention

L'inadaptation du niveau de sécurité par rapport aux risques encourus, tant au plan des dommages physiques que des malveillances, l'absence d'analyse préalable et le manque de cohérence dans les moyens de prévention sont souvent la cause

des sinistres (ex. : inefficacité de murs coupe-feu, mauvais fonctionnement des systèmes automatiques d'extinction d'incendie).

Dans l'appréciation de la prévention informatique, on doit prendre en compte tout autant le risque immatériel (les conséquences d'un sabotage) que le risque matériel (incendie ou phénomène naturel, tel que l'inondation, la tempête, l'ouragan, le poids de la neige).

L'auteur de l'étude retient deux sources de prévention, l'une à partir d'une approche méthodologique, l'autre à partir d'une approche juridique. *703*

L'approche méthodologique repose, selon les auteurs, sur l'analyse de divers facteurs de sécurité d'information :

a) liés à l'organisation de l'entreprise (structure des responsabilités, impact de la réglementation) ;

b) liés à la sécurité physique (incendie, dégâts des eaux, pollution, alimentation électrique) ;

c) liés à la sécurité du système d'exploitation (moyens de secours, sécurité des télécommunications, procédures de sauvegarde) ;

d) et liés à la sécurité « applicative » (procédures, contrôles).

L'approche juridique, dite subsidiaire, concerne la prévention par la législation sur le droit de l'informatique et par des législations sur la protection des droits des auteurs de logiciels et sur la fraude informatique.

Outre l'assurance, l'entreprise doit donc envisager une protection en réalisant un bilan de sécurité, c'est-à-dire l'établissement et la certification d'un schéma directeur de sécurité des systèmes d'informations en passant par les phases usuelles : analyse des risques, évaluation des risques maximum et audit des moyens de sécurité.