Document generated on 03/22/2025 8:35 a.m.

Assurances

Assurances

LES ASSURANCES CONTRE LE PIRATAGE INFORMATIQUE

Rémi Moreau

Volume 68, Number 4, 2001

URI: https://id.erudit.org/iderudit/1105349ar
DOI: https://doi.org/10.7202/1105349ar

See table of contents

Publisher(s)

HEC Montréal

ISSN

0004-6027 (print)
2817-3465 (digital)

Explore this journal

Cite this document

Moreau, R. (2001). LES ASSURANCES CONTRE LE PIRATAGE INFORMATIQUE. *Assurances*, *68*(4), 589–595. https://doi.org/10.7202/1105349ar

Tous droits réservés © Université Laval, 2001

This document is protected by copyright law. Use of the services of Érudit (including reproduction) is subject to its terms and conditions, which can be viewed online.

https://apropos.erudit.org/en/users/policy-on-use/

érudit

This article is disseminated and preserved by Érudit.

Érudit is a non-profit inter-university consortium of the Université de Montréal, Université Laval, and the Université du Québec à Montréal. Its mission is to promote and disseminate research.

https://www.erudit.org/en/

Assurances, volume 68, numéro 4, janvier 2001, 589-596

GARANTIES PARTICULIÈRES

par Rémi Moreau

LES ASSURANCES CONTRE LE PIRATAGE INFORMATIQUE

L'origine de l'assurance informatique

Nous avons déjà publié dans ces pages, au début de la décennie 1990, des commentaires sur l'assurabilité des systèmes informatiques contre les virus. À l'époque, nous n'avions en tête que les risques susceptibles de rendre amnésiques les millions d'ordinateurs dans le monde. Nous avions également passé en revue les principaux marchés d'assurance à cet égard.

La définition du virus informatique, il y a dix ans, était beaucoup plus restrictive que maintenant. Qu'on en juge par la définition de l'époque : « intrusion parasite glissée dans une disquette et qui, introduite dans l'ordinateur, anéantit son unité centrale et contamine ou détruit totalement ou partiellement les programmes ».

Généralement, on pouvait alors dénombrer sur les marchés spécialisés d'assurance quatre types de polices :

- Assurance des biens : la garantie dite « tous risques » était limitée à l'endommagement physique ou tangible des biens assurés (ordinateurs ou logiciels), incluant les actes de malveillance, de vandalisme ou de sabotage. Sauf négociée au cas par cas, la garantie ne couvrait pas les dommages financiers inhérents à la contamination de programmes, que les biens soient physiquement endommagés ou non.
- Assurance des risques frauduleux : les Lloyd's avaient mis sur le marché, dans la décennie 1980, un formulaire conçu spéeialement pour couvrir les institutions financières contre la fraude informatique. Les garanties offertes complétaient

les protections que l'on retrouve usuellement dans les polices D.D.D. Cette assurance (Electronic Computer Crime - E.C.C) garantissait l'assuré contre les dommages financiers résultant directement d'actes criminels commis à l'aide de systèmes électroniques et les différentes formes de malhonnêteté que l'opération électronique pouvait prendre (transferts de fonds et de valeurs, entrées comptables frauduleuses, versements faussement crédités). D'autres marchés offraient des garanties globales, y compris le cas d'intrusion malhonnête venant de l'extérieur, mais elles étaient conçues spécialement pour les institutions financières. Peu d'entreprises commerciales ou industrielles étaient intéressées par ces nouveaux risques assurables.

- Assurance malhonnêteté des employés : la police traditionnelle, dite D.D.D. (Détournement, Disparition, Destruction), applicable aux pertes pécuniaires causées par les actes malhonnêtes des employés de l'assuré, était de peu d'utilité vu l'exclusion relative à la fraude ou la malhonnêteté tirant leur origine à l'extérieur de l'entreprise.
- Assurance de responsabilité civile générale : cette assurance était susceptible de couvrir la réclamation d'une tierce personne contre un fabricant, contre un consultant, ou encore contre une entreprise de service fondée sur des dommages tangibles à des tiers, incluant la perte d'usage en cas de disparition accidentelle des informations contenues dans un disque dur.

On pouvait ainsi observer, il y a dix ans, que le virus informatique était un risque acceptable, mais restreint aux conditions restrictives ci-dessus énoncées.

L'assurance des risques criminels au tournant du millénaire

Comme autrefois, le virus informatique résulte essentiellement d'actions ou d'intrusions criminelles, frauduleuses ou malhonnêtes conçues pour paralyser ou simplement déjouer le parc micro-informatique d'un pays, d'une ville ou d'une entreprise publique ou privée. Toutefois, le virus ne s'attaque plus seulement à l'ordinateur, mais à l'ensemble des technologies de l'information qui ont cours actuellement sur la planète. Des événements comme le virus ILOVEYOU ou Melissa, qui s'attaquent essentiellement au réseau Internet, ont obligé les assureurs à prévoir des garanties

susceptibles d'indemniser les conséquences financières, même en l'absence de dommages matériels.

On estime que les entreprises, dans le monde, perdraient 1 500 milliards de dollars uniquement en cette année 2000, à cause des virus informatiques diffusés par Internet ou propagés par les E-Mail.

Heureusement, le « Love Bug », rapporté le 4 mai 2000, qui a contaminé essentiellement les réseaux courriel de quelque 45 millions d'utilisateurs, ne s'est pas infiltré dans les dossiers de traitement de texte, car les coûts auraient été astronomiques. On rapporte qu'actuellement ce piratage a coûté environ trois milliards de dollars aux entreprises touchées : pertes d'exploitation, coûts d'élimination du virus du système, coûts de réparation. Ce virus fut suivi de près par un second, Newlove.A, survenu le 19 mai, tout aussi violent, car son dossier attaché, lorsqu'ouvert, était en mesure de détruire tous les dossiers se trouvant sur le disque dur et non seulement la mémoire vive.

Le risque informatique a évolué sur deux plans : il s'attaque non pas tant aux appareils mais aux sites web, risquant ainsi une contamination du système de communication dans son ensemble ; il couvre toute intrusion criminelle dans un réseau informatique, sans que des dommages tangibles soient constatés. Les assureurs doivent sortir des scénarios classiques liés aux assurances de bris de machines, dont la couverture est réservée strictement aux dommages matériels et des dommages immatériels consécutifs aux dommages matériels.

Mais quels risques de dommages financiers (dits immatériels) couvre-t-on ? Principalement, les frais de reconstitution du système et les pertes financières qui en découlent, tels la perte d'exploitation, l'arrêt de travail ou de production en raison de défaillance bureautique ou l'interruption de la prestation de services, mais aussi l'ensemble des frais inhérents à la perte de contrats ou à la détérioration de l'image de marque d'une entreprise.

Internet peut même devenir un amplificateur de crise, car, en cas de désastre naturel ou technologique, on peut retrouver non seulement sur le Net des conseils en cas de crise, mais aussi, à l'inverse, des informations erronées, contre-information ou désinformation. Les entreprises ont donc intérêt à être garanties, dans le cadre de leurs lieux et opérations, contre la responsabilité civile découlant de l'utilisation de leurs produits ou de renseignements

erronés faits au public. À cet égard, uniquement les frais de défense, en cas de poursuites, peuvent être faramineux.

Les assureurs actuels, tels ACE, AIG, AXA, CGU ET CHUBB, utilisent différentes approches (voir *L'Argus* – 16 juin 2000) : soit la mise en place d'un produit spécifique (ACE propose le contrat« Dataguard ») couvrant toutes les conséquences découlant des actes de malveillance (reconstitution de l'information, frais supplémentaires, interruption d'affaires, fraude, détournement, extorsion, atteinte à l'image corporative). De son côté, Chubb offre l'assurance « Avant Garde », destinée aux petites et moyennes entreprises, qui conjugue l'assurance de responsabilité civile générale et l'assurance de responsabilité des administrateurs et des dirigeants ainsi que la garantie des actes frauduleux générant des pertes d'exploitation. AXA, au contraire, n'offre pas un produit distinct. Les garanties sont ajoutées, au cas par cas, et selon les besoins, par avenants joints aux garanties actuellement souscrites par les entreprises.

Le marché d'assurance londonien n'est pas en reste. Le National Computing Centre, la plus grande organisation britannique d'utilisateurs d'informatique, a établi, selon une étude, que le coût moyen d'élimination des virus était de 3 690 livres, mais qu'il pouvait s'élever jusqu'à 10 000 livres dans certains cas difficiles. L'étude observe aussi que les pirates extérieurs provoquent des dégâts pouvant avoisiner 15 000 livres pour chaque raid réussi, sans compter la perte de productivité qui s'ensuit. Enfin, la perte de réputation d'une entreprise se traduit par un abandon de sa clientèle au profit de ses concurrents. Aussi, 92 % des entreprises, selon des études récentes, démontrent qu'elles sont connectées à Internet ou disposent d'une messagerie électronique externe.

Forts de ces renseignements, nous avons répertorié quelques initiatives d'assurance britanniques. Le souscripteur de « Cyberliability », Hiscox, offre une protection financière de responsabilité civile et contre les pertes internes dérivant de Internet, du courrier électronique, d'extranet ou de l'utilisation du web. De plus, conjointement avec le courtier Alexander Forbes, il a lancé un dispositif de devis en ligne pour la distribution informatique de ce produit, sur le site www.cyberreliability.co.uk/insurance.

Les Lloyd's eux-mêmes ne sont pas en reste. Ils proposeraient bientôt aux sociétés qui disposent de navigateurs (Navigator, Explorator) ou aux clients d'une société de sécurité informatique une police d'assurance couvrant jusqu'à concurrence de 100 millions de dollars contre les dégâts provoqués par les *hackers*,

les pirates de l'ordinateur. Cette assurance intéresserait certainement des clients comme Yahoo, mais non des utilisateurs en particulier.

Le commerce électronique aux États-Unis rapporterait environ 6,5 milliards de dollars cette année, une véritable manne. Un autre rapport est encore plus spectaculaire : le e-commerce rapporterait 2,8 trilliards de dollars en l'an 2003. On y a dénombré 100 millions d'internautes à la fin de l'année 1999, soit la moitié des utilisateurs dans le monde. Selon un rapport du FBI fondé sur les réponses de 643 grandes entreprises américaines, on assiste actuellement à une véritable épidémie de criminalité informatique. En juillet, deux jeunes new-yorkais, dont un lycéen de 15 ans, étaient arrêtés par les autorités policières, soupçonnés d'avoir piraté des ordinateurs de la NASA, l'un pour avoir fait apparaître le message « *SSH is coming* », SSH désignant son nom de code : « *Sesame Street Haxorz* », l'autre pour avoir utilisé son ordinateur personnel afin de pirater deux ordinateurs du Laboratoire de propulsion par réaction de la NASA, à Pasadena, en Californie.

Aux États-Unis, comme ailleurs sans doute, les experts développent non seulement des programmes axés sur des garanties, mais aussi sur des moyens d'encryptage et de prévention (*virus-detection technology*). Il est d'abord essentiel que les systèmes de communication électronique soient dotés de mots de passe, de clés et de cartes informatiques. On dénombre aussi de nombreux antivirus, mais le problème n'est pas tant leur manque de fiabilité que leur rapide désuétude devant un virus postérieur au logiciel de prévention.

Pour ce qui est des stratégies actuelles d'assurance aux États-Unis, les assureurs, tels AIG ou AIU, offrent des programmes traditionnels amendés, notamment des polices dites tous risques couvrant la contamination par virus du matériel informatique de l'entreprise, les dossiers informatiques et la perte d'exploitation qui en découlent.

Devant les risques de poursuites de plus en plus nombreuses, l'assurance de responsabilité civile est également modifiée pour couvrir les responsabilités de l'entreprise suite à des événements de piratage et de fraude informatique. La garantie des préjudices personnels ne manque pas de comprendre les actes de piratage et d'intrusion dans la vie privée et de violation des droits relatifs à la propriété intellectuelle. La garantie des dommages matériels à autrui comprend non seulement les dommages tangibles aux biens,

y compris la perte d'usage, mais aussi la perte d'usage de biens non endommagés.

La science de la gestion dees risques n'est pas en reste. Dans un article intitulé *Integrated Risk Management in the Internet Age* (La gestion intégrée des risques à l'ère Internet), par Luis Ramiro Hernandez (June 2000/Risk Management), l'auteur précise qu'il devient notoire que les nouvelles technologies de l'information drainent avec elles leur lot de nouveaux risques, qu'il est nécessaire d'abord de définir, puis de maîtriser :

> « In addition to natural and man-made disasters, human errrors, and hacker and virus attacks, the continued growth of the Internet and network computing is breeding new categories of peril. Information theft, malicious code, denial of service and access violations threaten companies worlwide. No matter what the source may be, businesses today cannot affford the interruptions these events cause. »

L'auteur explique que la gestion intégrée des risques peut aider à réunir toutes les ressources potentielles de l'entreprise afin de contrer ces nouveaux risques. Les gestionnaires commencent à développer des techniques qui reposent sur l'ensemble des risques susceptibles d'affecter l'entreprise : risques de crédit, risques de marché, risques d'affaires, risques organisationnels. La première étape consiste à unir ou rendre les différents risques homogènes. Une fois que les canaux de liaison sont ouverts, la détection rapide des risques est facilitée par des programmes de formation du personnel et des procédures et des pratiques de surveillance. L'intégration, l'interaction et la communication entre les différentes disciplines permettent, entre autres aspects, de normaliser les procédures de contrôle, de resserrer les liens entre la direction et les cadres, de mieux mesurer les risques, et de réduire les coûts par la mise en commun des ressources budgétaires.

Des compagnies comme IBM, par exemple, ont su tirer profit au maximum des possibilités de lier ensemble les risques traditionnels et les risques liés à la nouvelle économie, d'assurer la confidentialité des données et de mieux prévenir l'accès non autorisé aux informations privilégiées.

Une nouvelle garantie contractuelle informatique

La Société française Adhersis a annoncé son intention, en octobre dernier, de s'installer au Québec, qui sera le siège social en

Amérique du Nord de cette société de stockage et d'encryptage contre la perte, le piratage ou la destruction de données informatiques. La société Adhersis gatantit par contrat la résurrection des données perdues ou détruites.

Des bureaux régionaux seraient ouverts dans cinq villes canadiennes au cours des deux prochaines années. Le système de stockage de cette société se veut à toute épreuve. Il encrypte les renseignements qu'il reçoit, les compresse et les envoie dans un bunker spécialisé, dont l'emplacement exact est gardé secret. Seul le client détient la clé d'encryptage de l'information.

Le système peut être utilisé par les ordinateurs et les téléphones sans fil, lorsqu'ils sont reliés au centre de sauvegarde par Internet.