DOSSIER 2013

VERZEKERINGEN EN INFORMATIE- EN COMMUNICATIETECHNOLOGIEËN

ASSURANCES ET TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Coordination / Coördinatie: Charles-Albert van Oldeneel
Rédacteur en chef du Bulletin des Assurances
Hoofdredacteur van het Tijdschrift voor Verzekeringen

Kluwer
a Wolters Kluwer business

Nog te verkrijgen / Encore disponibles:

Dossier 11, 2005, Assurances et droit fiscal
Verzekeringen en fiscaal recht

Dossier 13, 2007, Discrimination, différenciation hommes/femmes et assurances
Discriminatie, geslachtsdifferentiatie en verzekeringen

Dossier 14, 2008, Levensverzekeringen en giften
Assurances Vie et libéralités

Dossier 15, 2009, Solvency II & IFRS

Dossier 16, 2010, De informatieplicht in verzekeringen / Le devoir d'information en assurances

Dossier 17, 2011, Réforme du contrôle du secteur financier *(Twin Peaks)*
Hervorming van het toezicht op de financiële sector *(Twin Peaks)*

Dossier 18, 2012, La compliance en assurance
Compliance in verzekering

www.bulletindesassurances.be
www.tijdschriftvoorverzekeringen.be

De teksten uit dit tijdschrift worden ook online gepubliceerd op **Jura** en **Jura Notariaat**.

Les textes de cette revue sont également publiés en ligne sur **Jura** et **Jura Notariat**.

Dossier-Tijdschrift voor verzekeringen / Bulletin des assurances

Uitgegeven door:

Kluwer

Verantwoordelijke uitgever:
Hans Suijkerbuijk
Motstraat 30
2800 Mechelen

Klantenservice Kluwer:

Tel.: 0800 40 300 (gratis oproep)
info@kluwer.be

ISBN: 978-90-46-55889-8

Édité par:

Kluwer

Éditeur responsable:
Hans Suijkerbuijk
Drève Richelle 161 L
B-1410 Waterloo

Service clientèle:

Tél.: 0800-40 330 (appel gratuit)
info@kluwer.be

ISBN: 978-90-46-55889-8

INHOUDSTAFEL / TABLE DES MATIERES

DE AUTEURS / LES AUTEURS

Jean-Christophe ANDRÉ-DUMONT	Head of Legal and Compliance Allianz Life Luxembourg S.A.
Anne CATTEAU	Avocate au Barreau de Bruxelles
Jos DUMORTIER	Advocaat time.lex
Hervé JACQUEMIN	Chargé d'enseignement à l'Université de Namur (CRIDS) Chargé de cours invité à l'UCL Avocat au barreau de Bruxelles
Thierry LÉONARD	Avocat au Barreau de Bruxelles Professeur à l'Université St Louis-Bruxelles
Sandra LODEWIJCKX	Avocate au Barreau de Bruxelles
Claude RAPOPORT	Administrateur Délégué Portima S.C.R.L.
Sofie STEVENS	Bedrijfsjurist FVF
Patrick VAN EECKE	Prof. Faculteit rechten Universiteit Antwerpen Visiting Professor, Queen Mary University of London Visiting Lecturer, King's College, London Advocaat aan de balie van Brussel
Charles-Albert VAN OLDENEEL	Juriste d'entreprise Assuralia

Risques cybernétiques: notion et couvertures

Sandra Lodewijckx
et
Anne Catteau (1)

(1) Les auteurs remercient Max HERMUS pour sa précieuse collaboration.

of haar verzekeringspolis voldoende bescherming biedt. Indien dit niet het geval is, is een verzekering tegen cyberrisico's het beste wapen.

RÉSUMÉ

À l'heure actuelle, les entreprises dépendent dans une large mesure des technologies de communication et des possibilités qui leur sont offertes par Internet ou d'autres réseaux d'informations. En outre, les entreprises et les organisations stockent une quantité sans cesse croissante de données et la problématique de la protection des données (informations sensibles ou non) occupe de plus en plus souvent le devant de la scène.

Les risques dits cybernétiques se présentent tant à l'intérieur de l'organisation, où ils résultent des processus et entraînent souvent des dommages matériels, qu'à l'extérieur de l'organisation, en particulier les risques de dommages qui sont transférés, par des tiers, principalement par le biais de l'Internet, et qui ont souvent uniquement des conséquences immatérielles.

Cela étant dit, la question se pose de savoir si les entreprises belges sont suffisamment armées contre ces risques cybernétiques.

Les assurances de dommages (dites 'first party') que souscrivent les entreprises couvrent généralement les dommages matériels causés aux biens de l'entreprise (bâtiments, machines et éventuellement matériel informatique). Les programmes informatiques (logiciels) et les données ne sont souvent pas inclus dans la couverture. En outre, l'organisation doit pouvoir prouver les dommages matériels ou physiques pour pouvoir prétendre à une indemnisation.

Les assurances de responsabilité (dites 'third party'), comme l'assurance R.C., offrent une couverture plus étendue, étant donné qu'elles couvrent les dommages immatériels.

Les assurances qui ciblent spécifiquement les risques cybernétiques offrent des couvertures de deux types: la responsabilité de l'entreprise et les dommages propres qu'elle pourrait subir. Elles couvrent la responsabilité civile pour toutes les plaintes de tiers suite à une infraction à la confidentialité des données personnelles ou commerciales. Elles englobent également une couverture de la responsabilité en ce qui concerne la sécurité du réseau: lorsque l'accès au réseau est temporairement suspendu en raison d'un virus, lorsque des dommages sont causés au réseau de tiers... Ces assurances couvrent aussi souvent les frais réalisés dans le cadre de la 'responsabilité publique' de l'entreprise ou en cas de management de crise, ainsi que les frais qui sont réalisés en vue de remédier aux atteintes à la réputation des dirigeants d'entreprise. Enfin, les frais de notification à l'intéressé dont les données ont été piratées et/ou aux autorités publiques sont également souvent couverts.

Certaines polices en matière de risques cybernétiques prévoient une couverture des dommages propres causés à l'organisation. Dans ce cas, les frais de restauration du réseau suite à une interruption ou une attaque (frais de contrôle et de surveillance, frais de réparation et de restauration des données) sont couverts. Les pertes d'exploitation dues à une interruption des activités sont en général couvertes, mais pour une durée limitée.

Dans un monde où la communication s'effectue en grande partie par voie électronique, les entreprises disposant d'une couverture d'assurance adaptée sont plutôt rares. Il est dès lors recommandé à toute entreprise qui est exposée à des risques numériques d'examiner si sa police d'assurance lui offre une protection suffisante. Si ce n'est pas le cas, une assurance contre les risques cybernétiques constitue la meilleure arme.

INTRODUCTION

Dans le monde actuel, presque toutes les entreprises dépendent des technologies de la communication, et des services délivrés par internet ou d'autres réseaux d'informations. L'ampleur de ce phénomène ne cesse de croître. Les entreprises stockent de plus en plus de données, qu'elles soient sensibles ou non, notamment dans le cadre du commerce en ligne. En sus, les développements tels que le *cloud computing* entraînent une dématérialisation totale de la possession de ces données.

La fréquence et la gravité des pannes de système et des vols de données augmentent à un rythme alarmant ces dernières années.

Cependant, l'on constate en pratique que la plupart des entreprises ignorent si leurs polices d'assurance couvrent ou non les risques cybernétiques.

Selon une étude menée en 2012 (2), alors que 99% des entreprises européennes ont, au cours des cinq années écoulées, subi des pertes qu'elles jugent imputables aux risques informatiques et cybernétiques, 38% d'entre elles pensent que les risques informatiques sont couverts par l'assurance pertes d'exploitation, alors que, dans la pratique, il s'avère que les assurances pertes d'exploitation classiques ne prennent pas – ou trop peu – en compte la grande diversité de risques informatiques et cybernétiques.

Le présent article s'articulera donc en trois volets. Nous tenterons tout d'abord de délimiter cette notion de 'risque cybernétique'. Nous proposons ensuite d'analyser la couverture que les assurances dites classiques offrent pour les risques cybernétiques. Enfin, nous aborderons les produits créés par le marché pour couvrir spécifiquement ce type d'aléa.

Le concept de risque cybernétique

Qu'entend-on tout d'abord par 'risque cybernétique'? Les risques cybernétiques et la responsabilité qui en découle, concernent essentiellement des dommages immatériels. C'est généralement à des droits immatériels qu'il est porté atteinte (droit d'auteur, droits de la personnalité, droit au respect de la vie privée, réputation...).

L'on distingue traditionnellement le risque cybernétique interne du risque cybernétique externe.

(2) ACE European Risk Briefing 2012, IT and cyber risk.

Risque cybernétique interne

Le risque cybernétique interne vise les risques qui viennent de l'intérieur de l'entreprise: manipulation de données ou hacking interne commis par les employés, les administrateurs, les consultants... De simples erreurs humaines peuvent parfois être lourdes de conséquences. Ces risques peuvent mais ne sont pas essentiellement véhiculés par internet.

Les conséquences de ces risques peuvent être matérielles: des appareils (hardware et software) peuvent être volés, ou peuvent être volontairement endommagés. Les conséquences les plus importantes se situent toutefois au niveau des dommages immatériels: même en interne, des données peuvent être subtilisées, peuvent être utilisées de manière erronée, des matériaux protégés par le droit d'auteur peuvent être piratés...

Les dommages immatériels qui en résultent peuvent également être causés à des tiers, dès lors par exemple que les données personnelles de clients ou de relations sont subtilisées.

Risque cybernétique externe

Sont ici visés les risques de dommages véhiculés par des tiers, essentiellement cette fois-ci par l'intermédiaire d'internet. Il s'agit des assauts d'hacking externe, mais aussi parfois des interruptions de courant lors d'opérations importantes, qui peuvent par exemple entraîner une perte de données.

Ils auront généralement uniquement des conséquences immatérielles: dommages causés à l'entreprise elle-même tels que le vol de connaissances, une infraction aux droits de propriété intellectuelle, une désorganisation pouvant aller jusqu'au dommage de réputation, la violation de données personnelles des employés, frais supplémentaires de sécurisation, de communication, de défense... La responsabilité de la société pour non-exécution de certaines obligations peut parfois être mise en jeu. Il peut s'agir parfois également de dommages à des tiers (violation de données personnelles stockées et traitées par l'entreprise).

Étendue du risque

Les risques IT et cybernétiques peuvent être extrêmement variés. Du simple effet d'une erreur humaine, comme l'oubli d'un portable dans un train, à l'hacktivisme à large spectre ou le cyber-espionnage. Ils peuvent également être très étendus et ont toujours des conséquences coûteuses pour les entreprises.

De manière générale cependant, les entreprises évaluent le risque cybernétique avec beaucoup de clémence. Selon l'étude menée par ACE, ce risque vient seulement en quatrième position des préoccupations des entreprises, après le risque terroriste, le risque environnemental et le risque à l'exportation. En revanche, il est classé comme deuxième risque émergent par les grandes multinationales.

Une autre étude, menée fin 2012 (3), démontre qu'en 2012, 60.000 crimes cybernétiques ont été enregistrés en Allemagne. En réalité, seul un crime cybernétique sur mille est reporté aux autorités. Les cyber-risques et leurs conséquences sont de manière générale très largement sous-estimés par les entreprises. Seuls 6 pour cent des experts d'Allianz estiment que leurs clients sont conscients de ces risques.

Une heure d'interruption de production/business peut résulter en un dommage allant de 100.000 euros à 3 millions d'euros, en fonction de la taille de l'entreprise et de la façon dont son business a été affecté. C'est ce qui ressort d'une autre étude menée par Allianz (4).

Lors d'un 'Cyber Risk Survey', il est apparu en 2013 (5) que 54% des répondants se disaient avoir été victimes d'une attaque cybernétique au cours des trois dernières années, là où en 2012 seuls 25% des répondants étaient dans ce cas. 76% de répondants se disent familiers avec les assurances des risques cybernétiques. Cependant, 60% des mêmes répondants avouent ne pas avoir conclu d'assurance spécifique contre de tels risques.

Sanctions en droit belge

En droit belge, les délits liés au cyberespace font l'objet de sanctions à plusieurs niveaux.

Au niveau pénal tout d'abord, la loi du 28 novembre 2000 relative à la criminalité informatique a inséré de nouvelles dispositions dans notre Code pénal, visant à réprimer certains délits liés à l'espace cybernétique. Ainsi, les notions de faux en informatique, de fraude informatique et de hacking ont fait leur entrée dans le Code pénal.

Le faux en informatique (article 210*bis* C. pén.) consiste en la falsification de la réalité via manipulation de données. Il est puni d'une peine de prison de 6 mois à 5 ans et/ou d'une amende de 156 euros à 600.000 euros.

La fraude informatique (article 504*quater* C. pén.) vise l'opération consistant à chercher à se procurer un avantage économique illégal via la manipulation de données; elle est également réprimée d'une peine de prison de 6 mois à 5 ans et/ou d'une amende de 156 euros à 600.000 euros.

Le hacking (article 550*bis* C. pén.) consiste à obtenir un accès non autorisé à un système informatique. Le hacking externe est également puni d'une peine de prison de 3 mois à 1 an et/ou d'une amende de 156 euros à 150.000 euros. Le hacking interne est encore plus gravement considéré puisqu'ici les peines de prison peuvent aller de 6 mois à 2 ans et/ou une amende peut être infligée de 156 euros à 150.000 euros.

Au niveau civil, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ('Loi vie privée') a pour but la protection des données personnelles. Elle confère des droits aux individus

(3) Allianz Cyber Protect for a secure digital corporate future.
(4) Allianz Expert Risks Articles, IT Risks – Cyberspace attacks.
(5) Marsh 2013 Cyber Risk Survey.

dont les données personnelles sont traitées, et impose des obligations au responsable du traitement de ces données.

La loi du 13 juin 2005 relative aux communications électroniques ('Loi communications électroniques') a transposé en droit belge la directive européenne 2009/136. Cette loi impose des obligations spécifiques de notification pour les fournisseurs publics de services de communications. En cas d'atteinte aux données personnelles, ces fournisseurs devront notifier cette atteinte aux autorités nationales compétentes, et à leurs abonnés si l'infraction a des conséquences défavorables pour ces derniers.

Enfin, notons que le Parlement européen a déposé le 25 janvier 2012 une proposition de règlement pour la protection des données personnelles (appelé 'Règlement E-Privacy). Cette proposition comporte de nouvelles obligations pour les entreprises (désignation d'un Chief Privacy Officer pour les grandes entreprises), obligations d'information plus poussées, parmi lesquelles l'obligation d'informer les individus en cas de violation de leurs données. Ce nouveau règlement européen entraînera donc certainement une responsabilité accrue des entreprises qui manipulent des données personnelles. L'on s'attend à ce que ce règlement soit adopté dans le courant de l'année 2014, pour une entrée en vigueur en 2016.

Que couvrent les polices traditionnelles?

Les risques liés à l'utilisation du cyberespace peuvent donc s'avérer divers et variés. Lorsqu'une entreprise identifie un risque, elle essaye généralement de se couvrir contre la survenance et/ou les conséquences de ce risque, soit en assumant ce risque en interne, soit par le biais de contrats d'assurances.

Aux Etats-Unis, où la percée des assurances contre les risques cybernétiques est pour l'instant plus significative qu'elle ne l'est en Europe, l'on identifie comme tendances influençant la conclusion d'une assurance cyber-risques notamment l'évolution législative. Outre-Atlantique, l'essor des assurances contre les risques cybernétiques est en effet grandement dû à la législation instaurant l'obligation de notifier publiquement les atteintes aux données personnelles *('mandatory notification of data breach')*. En Europe, la Directive ePrivacy de 2002 a subi en 2009 une modification importante, obligeant désormais les sociétés de télécommunications et les fournisseurs de services de communications électroniques accessibles au public à notifier les atteintes aux données personnelles. Le projet de Règlement E-Privacy (voy. ci-avant) pourrait étendre cette obligation à tous les secteurs.

Comme autre facteur, l'on retrouve également l'augmentation des menaces dues à l'essor des nouvelles technologies (ex.: smartphones, etc.), mais encore l'émergence du *cloud computing*, l'importance grandissante des médias sociaux…

Nous nous proposons d'analyser quelques-unes des polices les plus couramment conclues par les entreprises, et de voir dans quelle mesure ces dernières couvrent ou ne couvrent pas les risques cybernétiques. De manière globale, l'on constate que la plupart de ces polices, dites 'classiques' couvrent peu ou pas les risques cybernétiques, dans la mesure où elles exigent souvent la preuve d'un dommage matériel, dommage parfois bien difficile à prouver dans le cyberespace…

En effet, les deux formes les plus courantes de risque cybernétique sont les attaques (telles que le sabotage ou le hacking (6), le 'déni de service' (7), les invasions par des virus ou les actes de malveillance informatique (8)…) et les violations de données (qui peuvent résulter d'erreurs humaines, de hackers, d'employés ou de tiers volant ou ayant accès à des données personnelles). Or, ces deux types de risque entraînent parfois peu ou pas de dommages matériels.

Nous analyserons tout d'abord les polices dites *'first party'*, couvrant les dommages propres de l'entreprise, et ensuite les polices dites *'third party'*, couvrant la responsabilité des entreprises.

Assurances de dommages des entreprises

Couvertures courantes

Ces polices couvrent traditionnellement les dommages matériels aux biens de l'entreprise (bâtiments, machines, en ce compris éventuellement le matériel informatique), qui résultent de leur destruction (totale ou partielle), ou encore de leur perte (vol…). Ne sont généralement pas considérés comme biens couverts les 'équipements électroniques servant au traitement administratif de données', ou encore les 'supports informatiques d'équipements électroniques ainsi que les programmes qui y sont sauvés et les informations qui y sont sauvegardées'. La couverture de programmes informatiques (softwares) et de données est donc souvent exclue.

Par exemple, en cas d'attaque 'déni de service', le site web de l'entreprise doit temporairement être fermé, sans toutefois être endommagé de manière permanente. Il s'agit plutôt d'un dommage type 'pertes de revenus'. En cas de virus également, l'entreprise devra débourser des frais de nettoyage IT, mais le virus n'aura peut-être rien détruit, ni altéré de software.

Pour prétendre à une indemnisation, l'entreprise devra prouver un dommage matériel, tangible physiquement (sans toutefois parler de dommage corporel, bien entendu).

Sont souvent exclus les 'pertes, dommages ou aggravation de dommage, directement ou indirectement causés ou ayant le moindre lien avec l'abus de confiance, le détournement de fonds, la tromperie, le chantage'. L'intrusion intentionnelle dans le réseau de l'entreprise, le hacking, le vol ou la manipulation de données ne sont donc pas couverts.

---

(6) Entendu comme l'usage intentionnel et malveillant du site web d'une société, dans le but d'altérer ou de détruire ses données.

(7) Entendu comme le bombardement d'un site de millions d'e-mails, afin de bloquer temporairement l'accès au site par ses utilisateurs légitimes.

(8) C'est-à-dire tout usage malhonnête et intentionnel visant à atteindre le réseau d'une société: cheval de Troie (programme d'apparence inoffensif contenant une fonction illicite cachée, utilisé notamment pour pénétrer par effraction dans un ordinateur et consulter, modifier ou détruire des données) ou bombe logique (programme non reproducteur contenant une fonction cachée, nuisible et le plus souvent destructrice, et généralement associée à un déclenchement différé).

Exclusions courantes

En outre, ces polices excluent généralement automatiquement les dommages immatériels. Or, on l'a vu plus haut, les risques cybernétiques n'ont généralement que des conséquences non matérielles.

Assurance Tous Risques Informatiques ou Tous Risques Electroniques

Il s'agit d'une des premières assurances à laquelle l'on songe en parlant de risque cybernétique. Elle sert à protéger le propriétaire ou l'utilisateur de matériel électronique et informatique.

Les assurances Tous Risques Informatiques sont généralement des assurances dites 'tous risques sauf': c'est-à-dire qu'elles couvrent toutes les conséquences des risques non exclus dans la police. La philosophie de ce produit reste cependant toujours la même: elles couvrent uniquement les dommages provenant d'une cause extérieure au matériel (9).

Ces polices garantissent généralement uniquement l'indemnisation des dommages à des biens matériels. Certaines proposent toutefois des extensions de garantie telles que les frais pour reconstituer les informations perdues ou détruites à la suite d'un sinistre indemnisable. Les frais d'exploitation auxquels l'assuré doit faire face après un sinistre sont généralement également pris en charge (10).

Couvertures courantes

Les polices Tous Risques Informatiques couvrent donc généralement les dommages matériels apportés aux biens assurés, en tant que destruction physique, totale ou partielle, du matériel informatique et/ou électronique (écran qui implose, panne, défectuosité d'un appareil...).

Elles indemnisent également des frais supplémentaires. Parmi ceux-ci l'on retrouve les frais effectués pour la reconstitution des données perdues suite à un événement couvert (par exemple perte de données suite à une panne). Il s'agit ici également de dommages matériels: coût de ré-enregistrement des données, salaire du personnel, permanent et temporaire (analystes, programmeurs...), frais de location de locaux temporaires, coût de rachat de logiciels... La couverture porte uniquement sur l'indemnisation matérielle de la recomposition de ces données: elle ne comporte donc pas d'indemnisation de la valeur intrinsèque des données en elles-mêmes.

L'on retrouve également les frais supplémentaires d'exploitation: l'assureur prend en charge, pendant un laps de temps (généralement un an) la différence entre le coût du traitement informatique exposé par l'assuré après le sinistre et le coût supporté en temps normal. Il s'agit par exemple des frais encourus pour la location d'un matériel de remplacement de caractéristiques identiques à celui endommagé, des frais d'adaptation du programme informatique au matériel de remplacement, frais de personnel engagé à titre temporaire...

Enfin, les frais d'exploitation font parfois l'objet d'une couverture dans une police Tous Risques Informatiques: l'assureur garantit alors les pertes résultant de la diminution du chiffre d'affaires de l'entreprise, suite à la survenance d'un sinistre couvert.

Les assureurs requièrent souvent de leurs preneurs d'assurance qu'ils conservent une copie de leurs logiciels en dehors de l'entreprise ou dans des bâtiments distincts, et qu'ils procèdent à un back-up (hebdomadaire, journalier) de leurs données.

Exclusions courantes

Bien que ces dommages aient parfois une cause externe, les polices Tous Risques Informatiques excluent généralement explicitement les dommages qui trouvent leur origine dans les virus informatiques, ou l'altération ou la perte de données résultant d'une mauvaise manipulation ou programmation erronée (erreur humaine).

Les altérations ou pertes de données ou d'informations sans conséquences matérielles aux supports informatiques eux-mêmes sont aussi exclues.

En ce qu'elles ne couvrent que les conséquences matérielles des sinistres, et non les dommages immatériels résultant de pertes de données ou de l'intrusion de virus, les assurances Tous Risques Informatiques ne sont donc pas complètement adaptées pour se protéger des risques cybernétiques.

Assurance fraude

Les assurances fraude ont pour but principal de protéger l'entreprise contre les dommages résultant de fraude interne, par exemple commise par un collaborateur. La plupart des institutions financières (banques, entreprises d'assurance...), en raison de l'ampleur des fonds qu'elles manipulent, mais également de l'importance des données traitées au quotidien, ont conclu ce type d'assurance. Dans beaucoup d'autres secteurs cette assurance est quasi inexistante.

L'assurance fraude couvre les dommages financiers découlant d'une fraude commise soit en interne (par des employés de l'assuré, avec ou sans complicité), soit en externe (par des tiers, sans complicité interne), et qui mettrait à mal la continuité de l'entreprise. Ces polices considèrent comme actes frauduleux le vol, le détournement de fonds, l'escroquerie, l'abus de confiance, le faux en écriture (établissement de fausses factures, de fausses notes de frais), ou encore l'atteinte au traitement automatisé de données.

Même si les faux informatiques ou la manipulation informatique sont parfois visés, cette assurance n'indemnise généralement que les conséquences pécuniaires liées à l'utilisation de tels documents frauduleux. Les assurances fraude également ne sont donc pas totalement adaptées pour se protéger des risques cybernétiques.

(9) 'De polis informatica', *in* M. DE CLERCK et C. DE CLERCK, *Bedrijfsschade verzekeren*, Malines, Kluwer, 2006, pp. 280-285.

(10) E. THYS, 'Assurances techniques', *in* X, *Les entreprises et leurs assurances*, Waterloo, Kluwer, 2006, p. 268.

Assurance R.C. Exploitation

En matière de risque cybernétique, les assurances de la responsabilité, dites *'third party'*, offriront sans conteste la protection la plus étendue puisqu'elles apportent une couverture des dommages immatériels.

Couvertures courantes

L'objet de cette assurance est de garantir la responsabilité extracontractuelle de l'entreprise en raison de dommages causés à des tiers, et qui résultent de l'exploitation des activités de l'entreprise. La responsabilité contractuelle est couverte uniquement en cas de concours avec une responsabilité extracontractuelle.

On y retrouve les dommages corporels (atteintes à l'intégrité physique), matériels (destruction ou perte de biens), et immatériels (perte d'usage d'un bien ou d'un droit, privation de jouissance, perte de bénéfices ou autres pertes pécuniaires, perte de parts de marché, perte de renommée commerciale, perte de clientèle). Généralement, seuls les dommages immatériels consécutifs à un dommage corporel ou matériel sont couverts.

Les dommages immatériels non consécutifs sont ceux qui découlent d'un dommage corporel ou matériel non couvert par le contrat d'assurance, alors que les dommages dits 'immatériels purs' sont ceux qui ne découlent pas d'un dommage corporel ou matériel.

Ces deux types de dommages sont souvent exclus des assurances R.C. Exploitation; ils peuvent toutefois faire l'objet d'une couverture particulière, et il est alors souvent exigé qu'ils résultent d'un événement soudain, imprévu et involontaire dans le chef du preneur d'assurance.

Les risques couverts se définissent généralement comme ceux découlant de l'incendie, des troubles du voisinage, des atteintes à l'environnement, mais encore du recours à des sous-traitants ou du personnel mis à disposition du preneur d'assurance, ou des dommages occasionnés aux objets confiés au preneur.

Certaines assurances R.C. Exploitation offrent une couverture des dommages informatiques. Une police par exemple couvre 'les dommages occasionnés aux données informatiques ou la simple indisponibilité de ces données et toutes les conséquences qui s'ensuivent; les dommages causés par ou découlant de l'usage d'outils informatiques'. Elle exclut toutefois 'la responsabilité découlant des activités liées à l'usage d'internet, au développement, à l'entretien et à l'installation de softwares'.

Exclusions courantes

Les polices excluent généralement 'les dommages de toute nature causés aux supports d'information électronique ainsi qu'aux données qu'ils contiennent lorsque ces dommages résultent directement ou indirectement de l'utilisation de moyens de communication électronique, ainsi que ceux découlant de la pénétration du système par un virus'. Une police exclut en outre 'les dommages rendus possibles par le non-fonctionnement ou le dysfonctionnement de programmes, systèmes et/ou applications informatiques ou électroniques liés à une interpénétration erronée des dates'.

Elles excluent également souvent les dommages résultant d'actes de concurrence déloyale, ainsi que tout dommage découlant de l'atteinte portée à des droits de propriété intellectuelle tels que les brevets, les marques commerciales, les dessins et modèles ou encore les droits d'auteur.

Même si elles comportent généralement une couverture plus ou moins étendue des dommages immatériels et autres dommages résultant des pertes ou d'une baisse de l'exploitation, les assurances R.C. Exploitation ne couvrent généralement pas les risques qui pourraient être véhiculés par internet (hacking, virus...). En outre certaines excluent totalement les dommages immatériels consécutifs (par exemple les frais de notification d'une atteinte).

Assurance contre les risques cybernétiques

Malgré le fait qu'elles soient encore peu répandues dans notre pays, certains assureurs offrent déjà des assurances spécifiquement axées sur les risques cybernétiques. Le processus d'acceptation est toutefois généralement assez complexe. Les entreprises qui souhaitent conclure ce type d'assurance doivent fournir à leur assureur potentiel de nombreuses informations sur les mesures de sécurité qu'elles ont prises contre les cyber-infractions, ainsi que sur leurs processus internes. Les assurances contre les risques cybernétiques sont donc pour l'instant plus appropriées aux entreprises qui se sont déjà suffisamment protégées contre les risques cybernétiques.

La plupart des polices que l'on rencontre sur le marché belge offrent deux types de couverture: la responsabilité de l'entreprise et les dommages propres qu'elle pourrait subir. Rappelons que l'assurance des risques cybernétiques n'est pas un produit légalement réglementé; les dispositions de la loi du 25 juin 1992 sur le contrat d'assurance terrestre relative d'une part aux assurances de la responsabilité et d'autre part aux assurances de choses sont donc respectivement applicables. L'on songe ici aux spécificités telles que la couverture dans le temps, la couverture des frais de sauvetage...

Couverture de la responsabilité

Plusieurs types de dommages sont généralement couverts, qu'ils découlent de la responsabilité contractuelle ou extracontractuelle.

La responsabilité civile pour toutes les réclamations des tiers consécutives à une atteinte à des données personnelles ou commerciales est couverte. Sont visées toutes les violations de droits de propriété intellectuelle (droit d'auteur, plagiat, piraterie, détournement d'idées, concurrence déloyale...), ainsi que les cas de 'responsabilité multimédia': diffamation, calomnie, atteinte à la réputation. Les atteintes à la vie privée (vol de données de clients...) et à des informations confidentielles (secrets commerciaux...) et leurs conséquences sont également visées.

Les assurances contre les risques cybernétiques comprennent également souvent une garantie de la responsabilité liée à la sécurité des réseaux: accès au réseau rendu (temporairement) impossible suite à un virus ou autre, les dommages causés aux réseaux de tiers, la perte ou les dommages occasionnés aux données de tiers, le vol de codes d'accès aux systèmes de l'assuré, la divulgation de données par un employé.

Un autre volet important sont les dépenses liées à la 'responsabilité publique' ou à la gestion de crise.

Ainsi, sont couverts les atteintes à la réputation de la société et les frais relatifs à son rétablissement. Sont généralement ici visés les coûts et frais raisonnables qui ont été engagés pour contrôler et détecter toute utilisation impropre des données qui ont été affectées. Il s'agit tout d'abord des frais engagés pour le constat et l'établissement d'une violation de la protection de données, et pour la détermination de son origine.

Sont visés les frais de communication engagés dans le but de prévenir et/ou limiter toute atteinte à la réputation de l'entreprise suite à une cyber-attaque (frais de spécialistes et de conseillers indépendants en stratégie média, en relations publiques...). Les atteintes à la réputation individuelle sont aussi parfois indemnisées: il s'agit des frais parfois engagés en vue de réparer les atteintes faites à la réputation des dirigeants de l'entreprise et des personnes en charge du traitement des données (par exemple le directeur des services de l'information ou le directeur juridique).

Il faut noter que tous ces frais sont supportés par les assureurs, que l'atteinte à des données protégées soit réelle ou simplement alléguée. En effet, dans le monde virtuel, une allégation d'atteinte peut parfois causer tout autant de dégâts.

Enfin, les frais de notification aux personnes concernées, aux clients dont les données ont été violées et/ou à toute instance réglementaire lorsque ceci est exigé, rentrent en ligne de compte pour l'indemnisation.

Couverture des dommages propres

Les polices cyber-risques disponibles sur le marché belge ne couvrent pas toujours les dommages propres de l'entreprise. Certaines offrent cette possibilité en complément du volet responsabilité.

Sont alors couvertes les dépenses encourues dans la restauration du réseau suite à une interruption ou à une attaque (rachat d'un logiciel, sauvegarde (back-up). Les frais de monitoring et de surveillance sont parfois pris en charge, parfois pendant une période prédéterminée. Les frais de réparation et de restauration des données peuvent parfois être conséquents et seront à ce titre pris en charge.

Les pertes d'exploitation résultant d'une interruption des activités sont généralement couvertes par la garantie 'dommages propres': l'activité doit en effet parfois être temporairement (totalement ou partiellement) interrompue pour la constatation de la violation et la restauration d'une activité productive. Cette garantie est parfois limitée dans le temps (par exemple 120 jours après l'interruption).

La cyber-extorsion fait parfois l'objet d'une garantie en option: il s'agit de la couverture des demandes d'extorsion de fonds afin de mettre fin à une menace imminente (véridique ou alléguée) sur la sécurité du réseau de l'assuré, ou la dégradation d'un site web. Dans le même ordre d'idées, le cyber-vol peut aussi être indemnisé: il s'agit des pertes pécuniaires liées à un transfert non autorisé de sommes d'argent, commis par une source extérieure à l'entreprise.

Couverture du cloud computing?

Le *cloud computing*, à savoir l'accès, via un réseau de télécommunications, à des ressources informatiques partagées, entraîne un transfert de données vers le service en nuage, et comporte par là même une augmentation des risques: les données sont maintenant détenues par un tiers. Très peu de cyber-assurances couvrent le risque du *cloud computing*. Celui-ci est parfois inclus dans la définition de 'système informatique' ou de 'réseau'. Le cas échéant, un avenant peut venir combler cette lacune si nécessaire.

Services supplémentaires

Certains assureurs proposent, en sus de la couverture d'assurance proprement dite, des services connexes tels que la mise en place d'une hotline, les services de spécialistes de cyber-incidents, ou de cabinets d'avocats spécialisés dans l'assistance et l'accompagnement de victimes de cyber-attaques, ou encore des personnes actives dans la communication d'entreprise.

Conclusion

Rares sont aujourd'hui les entreprises qui peuvent se passer de la multitude de possibilités que leur offre le cyberespace. La plupart des entreprises actives dans le secteur tertiaire ont un site internet, plus ou moins développé. Celui-ci leur sert d'interface avec leurs clients. La majorité des communications se font aujourd'hui de manière électronique.

Les entreprises sont de plus en plus conscientes des atouts que le cyberespace peut leur fournir, mais des grands dangers qui l'accompagnent également. A l'heure actuelle cependant, peu d'entre elles disposent de mesures de protection adéquates. Ceci se passe malheureusement souvent à leur insu; la plupart des entreprises se pensent adéquatement protégées par leurs polices traditionnelles, alors que c'est parfois loin d'être le cas. L'assurance cyber-risque a donc certainement un bel avenir devant elle en Europe.

Dans ce contexte, nous pensons que les entreprises doivent se poser trois questions: *primo*, suis-je soumise à des risques cybernétiques, et ai-je pris des mesures internes de sécurisation pour me prémunir contre de tels risques? *Secundo*: les polices d'assurances que j'ai souscrites me protègent-elles suffisamment? Dois-je souscrire un produit adapté? Et *tertio*: mon entreprise est-elle préparée, en terme de moyens de gestion, à une crise cybernétique? Des plans de crise ont-ils été dressés? Tous les collaborateurs sont-ils au courant de la marche à suivre?

Ce n'est qu'après avoir passé ce test avec fruit, qu'une entreprise pourrait se targuer d'être suffisamment protégée pour être active dans le cyberespace...