Le prix du risque cyber

Didier PARSOIRE*
Sébastien HÉON**

Physionomie du risque : des invariants dans un monde en rapide évolution technologique

Qu'il s'agisse de vol de données (Marriott), de blocage des chaînes de production (Norsk Hydro) ou de *fake news*[1], les risques cyber semblent en pleine expansion, accompagnant l'essor des technologies de communication et l'interconnexion toujours croissante de réseaux et d'objets. Pourtant, dans cet univers technologique foisonnant et alors que les actifs immatériels prennent une place prépondérante, quelques lignes de force font figure d'invariants.

Motivation des attaquants

Les attaques informatiques, notamment les plus sophistiquées, sont réalisées par des personnes ou des organisations avec un objectif bien déterminé. Leurs motivations sont finalement classiques et obéissent très souvent à la classification MICE utilisée dans le renseignement : M (*money*), I (*ideology*), C (*coercion*) et E (*ego*). On pourrait y ajouter le C de « chance » car il existe encore des attaques informatiques opportunistes où le *hacker* découvre par hasard une vulnérabilité béante lui offrant un accès facile à des trésors numériques.

Il existe de nombreux exemples illustrant ces différentes motivations. Les très répandus *ransomwares* ou fraudes au président sont des illustrations parfaites de la motivation de gains financiers. L'idéologie et la coercition sont les moteurs puissants qui ont conduit à la formation de groupes d'attaquants comme les Anonymous ou les « armées cyber »

* Directeur Cyber Solutions, SCOR. Contact : DPARSOIRE@scor.com.
** Directeur adjoint Cyber Solutions, SCOR. Contact : SHEON@scor.com.

(Syrian Electronic Army[2], Iranian Cyber Army[3]). Souvent autoproclamés et non officiels, ces groupes visent ce qui représente à leurs yeux une opposition politique ou idéologique. Il ne faut pas les confondre avec les opérations cyber menées par des États qui, bien que motivées par des considérations géopolitiques, sont opérées dans un cadre bien défini. L'*ego*, finalement, se manifeste quand certains *hackers* révèlent publiquement des failles de produits très répandus comme l'iPhone, les PlayStation, ou les routeurs Cisco pour démontrer leur talent à la communauté des *hackers*.

Stratégies d'attaque

Pour arriver à leurs fins, les attaquants ont mis au point des stratégies qui, finalement, sont assez stables dans le temps. On peut citer la célèbre *Cyber Kill Chain*, théorisée par les chercheurs de Lockheed-Martin dès 2011 et qui reste d'actualité aujourd'hui. Les attaquants déroulent un plan en sept étapes adapté de la théorie militaire : reconnaissance de la cible, préparation des logiciels nécessaires à l'attaque, intrusion dans le système informatique, exploitation des vulnérabilités du système, installation de points d'accès spécifiques aux attaquants, établissement d'un canal de contrôle à distance, réalisation de l'attaque.

Ce schéma est indépendant des technologies utilisées par la cible et s'adapte à de très nombreux contextes. La multiplication des interconnexions et des outils de communication utilisés par la cible (réseaux sociaux, par exemple) va offrir aux attaquants de nombreux choix de canaux d'attaque. Sera choisi celui qui offre le meilleur retour sur investissement (facilité de mise en œuvre / étendue de l'attaque).

Par ailleurs, les attaquants obéissent à une logique économique en cherchant à maximiser leur gain et à minimiser leur investissement. Ils se tourneront donc vers les proies les plus faciles au sein de leur population cible.

L'exposition

L'exposition d'une entreprise, son attractivité pour les *hackers*, dépend davantage de son activité que des technologies qu'elle utilise. Bien sûr, plus l'entreprise est « connectée », plus les options d'attaque seront nombreuses. Mais, *in fine*, ce sont surtout la valeur des actifs et/ou le symbole ou l'image qu'elle véhicule qui attireront les attaquants : qu'elle soit traditionnelle ou en ligne, une banque sera toujours la cible des cybercriminels.

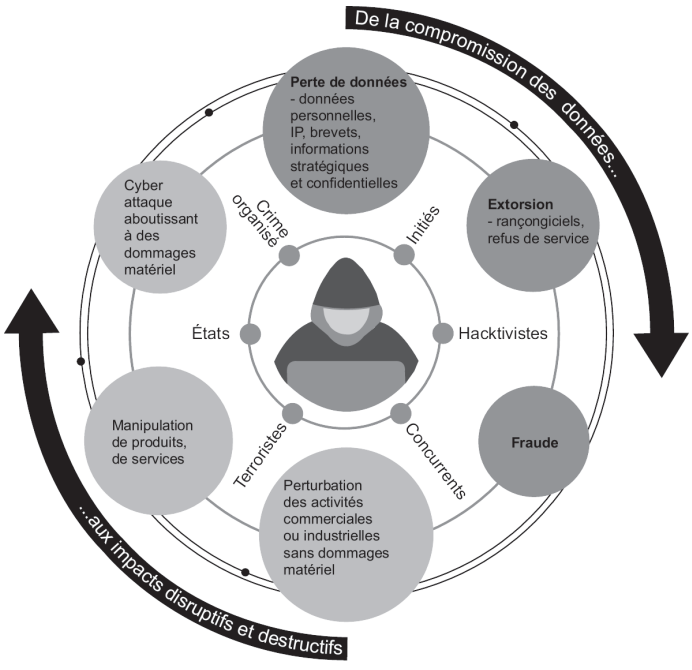
Toutefois, l'avènement du numérique a fait émerger des acteurs économiques au profil particulier : des entreprises relativement petites qui manipulent d'énormes quantités de données à caractère personnel : marketing digital, sites sportifs qui collectent les données des

montres connectées, *credit bureaus* dans le monde anglo-saxon, etc. Le rapport entre la taille de l'entreprise et la valeur de ses actifs (intangibles) est sans commune mesure avec celui des entreprises du monde tangible. Et à cause de leur petite taille, leur capacité à investir dans la protection de ces données est sans doute limitée. En conséquence, de nombreuses attaques ont touché ces acteurs ces dernières années : deux *credit bureaus* américains (Equifax en 2017, Experian en 2015), Orange en 2014 par le biais d'une petite agence de marketing, le site web MyFitnessPal de l'équipementier sportif UnderArmor en 2018.

Des impacts stables

Finalement, en bout de chaîne, les impacts des incidents cyber sont relativement constants et répondent en miroir aux motivations des attaquants. Nous en avons identifié six (cf. schéma *infra*) : la perte ou le vol de données, l'extorsion, la fraude, la perte d'exploitation (blocage des systèmes d'information), la manipulation malveillante d'un produit (introduction d'un virus dans une voiture connectée, par exemple), et les dommages matériels résultant d'incidents cyber.

Schéma
Six types de risque cyber



Source : SCOR.

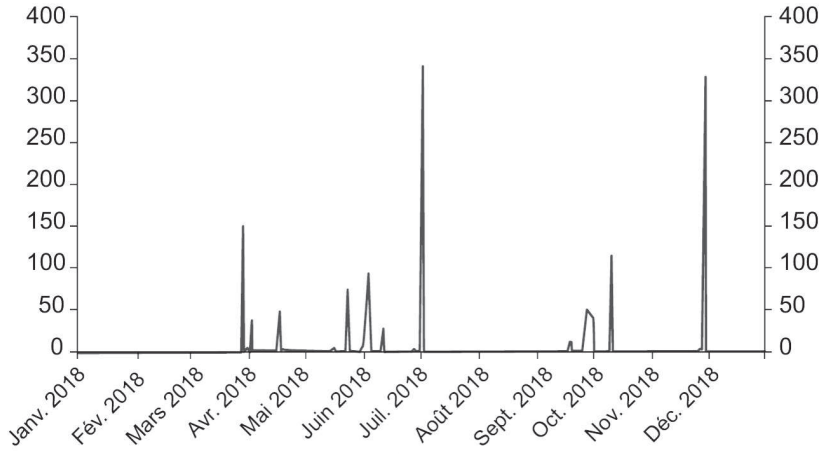
Au fil du temps, la pondération entre ces six types de risques évolue. Cette évolution dépend de la manière dont les attaquants peuvent monnayer le fruit de leurs attaques. En effet, depuis longtemps, les données personnelles, bancaires ou médicales sont très recherchées par les *hackers* qui les revendent à bon prix. À titre d'exemple, un numéro de carte bancaire avec le code de sécurité se revendait 5 dollars sur le *dark web* en 2017[4]. Ce *business model* est viable car la demande continue de stimuler l'offre. Mais, vraisemblablement, le cours des données volées s'effondrerait si d'importants volumes étaient mis soudainement sur le marché.

On constate d'ailleurs une évolution de certaines activités cybercriminelles. Depuis longtemps, les *ransomwares*[5] étaient des logiciels génériques, distribués le plus largement possible afin de contaminer le plus grand nombre possible d'ordinateurs. Dans cette logique de « pêche au chalut », le taux de retour est faible car peu de victimes paient finalement la rançon, la plupart utilisant leurs sauvegardes pour restaurer leurs données. Pour pallier cet inconvénient, les attaquants commencent à développer des *ransomwares* ciblés s'attaquant à une victime et la contaminant en profondeur (jusqu'aux sauvegardes). Il est alors beaucoup plus simple d'obtenir le paiement d'une rançon dans ce cadre. L'Agence nationale de sécurité des systèmes d'information (ANSSI) a d'ailleurs publié un rapport[6] sur le *ransomware* Lockergoga soupçonné d'avoir touché Altran et Norsk Hydro dans lequel ce nouveau *modus operandi* est analysé en détail.

Un risque de sévérité

Intuitivement, le risque cyber se divise en deux types d'impact : un « bruit de fond » assez stable dans le temps et de faible sévérité, auquel s'ajoutent des pics de sévérité élevés. Aucune base de données ne répertorie les incidents cyber de manière exhaustive, mais la législation américaine qui rend obligatoire la notification de toutes les pertes de données à caractère personnel donne un aperçu de ce profil de risque comme illustré ci-dessous. Le graphique 1 (*infra*) n'indique que le nombre de données perdues, pas les impacts financiers consécutifs.

Graphique 1
Nombre de données perdues ou volées aux États-Unis en 2018
(en millions)



Source : www.privacyrights.org/data-breaches.

L'APPROCHE TARIFAIRE DU RISQUE CYBER

Comment intégrer les caractéristiques du risque cyber dans une approche tarifaire ?

Les données disponibles aujourd'hui sur les impacts des incidents cyber sont limitées. Même dans le cas des pertes de données (cf. *supra*), le nombre de données perdues est disponible, mais les impacts financiers ne sont pas répertoriés. Les pertes d'exploitation, dues à des virus ou à des pannes, sont quant à elles très peu documentées car souvent passées sous silence par les victimes qui veulent éviter une mauvaise publicité. Finalement, seuls quelques grands incidents, les pics de sévérité, sont identifiés et encore souvent de manière approximative. La fréquence des incidents reste largement inconnue.

Par ailleurs, les canaux d'attaque disponibles (la surface d'attaque) s'étendent avec le développement des interconnexions. Ainsi, intuitivement, la fréquence des incidents est une fonction croissante du temps mais, cette loi aussi, reste inconnue. Cela rend le redressement des données historiques et la construction de scénarios « *as if* » très difficiles.

Construire un cadre basé sur l'expertise

Pour faire face à ces obstacles, la tarification du risque cyber pour une entreprise doit finalement s'appuyer sur ce que l'on connaît de ce risque. C'est pourquoi la recherche d'invariants et le jugement d'expert

sont fondamentaux à ce stade. Ils permettent de bâtir un cadre général de tarification dont la calibration s'améliorera au fur et à mesure que les données de sinistres s'accumuleront.

L'exposition d'une entreprise peut ainsi s'analyser selon trois axes invariants :

– son activité : il s'agit de sa « prédisposition génétique » au risque cyber : le degré de numérisation, souvent corrélé au secteur d'activité, les données qu'elle manipule, la ou les réglementations auxquelles elle obéit, son *business model* (B2B ou B2C, par exemple), la dispersion ou, au contraire, la centralisation de ses systèmes d'information. L'activité indiquera aussi comment analyser les pertes d'exploitation subies en cas d'incident informatique ;

– son attractivité pour les attaquants : il s'agit d'une combinaison de l'image ou du symbole que l'entreprise véhicule, des actifs intangibles qu'elle manipule, de son intérêt stratégique, des innovations qu'elle développe ;

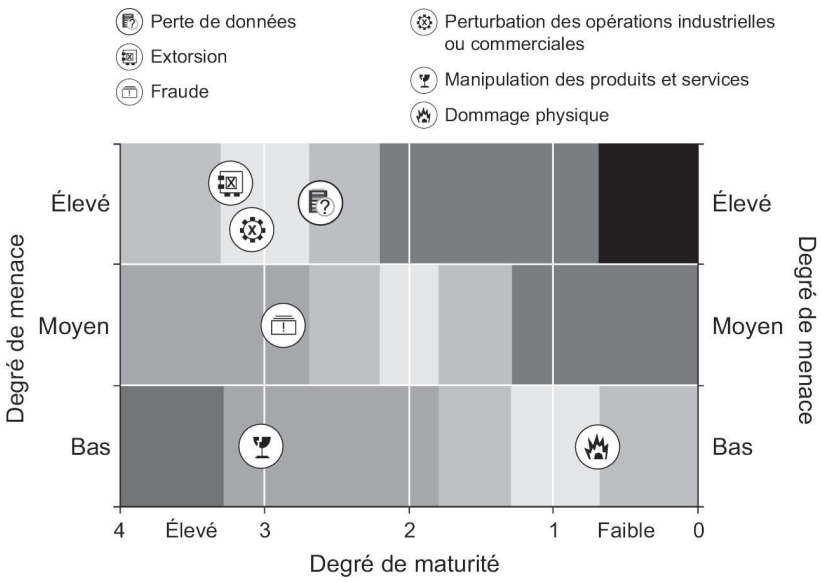
– sa maturité et sa résilience face au risque : la manière dont elle gouverne sa sécurité des systèmes d'information et notamment comment elle répartit ses efforts entre les outils technologiques de protection, les procédures de sécurité et les équipes.

De plus, la taille de l'entreprise est un critère important qui vient compléter l'analyse d'exposition. Cette taille revêt plusieurs aspects : le chiffre d'affaires, bien sûr, mais aussi le volume et la sensibilité des données manipulées, ou la dispersion géographique (une entreprise ayant de très nombreuses entités satellites offre une plus grande surface d'attaque qu'une organisation centralisée et monolithique).

L'exposition d'une entreprise s'appuie donc sur plusieurs critères objectifs et accessibles comme le chiffre d'affaires ou le secteur d'activité et sur le jugement d'expert pour l'évaluation de son attractivité et de sa maturité.

Cette exposition sera différente selon les six types de risque cyber considérés. Face à la perte de données, une entreprise de l'industrie lourde ne sera pas exposée de la même manière qu'un hôpital. On peut finalement combiner et représenter toutes ces informations sous forme de *heatmap* qui donne la fiche signalétique cyber de l'entreprise. Les six risques sont les bulles positionnées selon deux axes : la maturité en abscisse et le niveau de menace en ordonnée (cf. graphique 2 *infra*).

Graphique 2
***Heatmap* cyber**



Source : SCOR.

Des modèles fréquence-coût

L'analyse de sinistres est nécessaire pour construire et calibrer ces modèles mais le manque de données, en partie dû au faible taux de pénétration de l'assurance cyber, et de recul sur la sinistralité imposent une démarche graduelle et une segmentation fine des cas disponibles.

En effet, la structure de coût varie selon le type de risque : les six types de risque cyber ont des impacts financiers différents. Une perte de données, par exemple, engendre des frais différents d'une perte d'exploitation, eux-mêmes dépendant du secteur d'activité et de la taille de l'entreprise touchée. On ne peut donc pas rassembler tous les sinistres cyber répertoriés dans une seule population. Au contraire, il faut segmenter cet ensemble pourtant petit en échantillons homogènes.

La sévérité

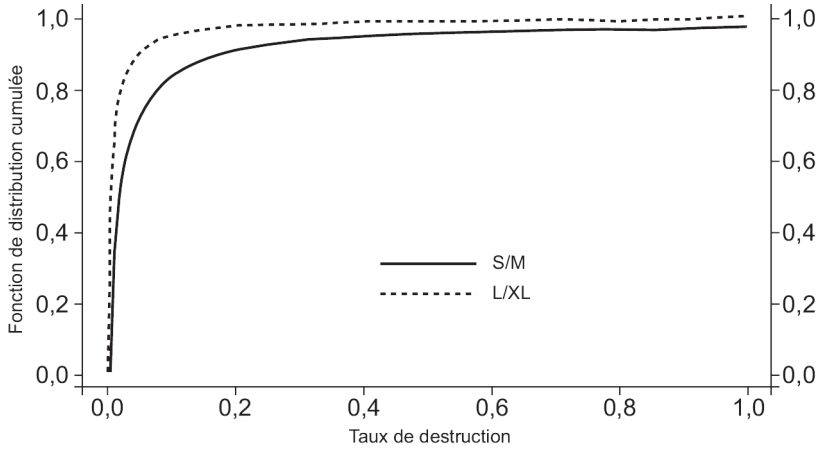
Comme évoqué plus haut, les pics de sévérité sont souvent rendus publics. Par exemple, plusieurs victimes des attaques NotPetya et WannaCry de 2017 ont communiqué des estimations d'impacts, comme FedEx qui évoque une perte de 300 M$ dans son rapport financier[7]. Quant aux pertes de données, Target a indiqué[8] que

l'attaque dont le groupe a été victime en 2013 avait atteint en mai 2017 la somme de 202 M$.

Ces chiffres donnent des points de référence qui doivent être analysés relativement à la taille de l'entreprise. En effet, pour Target, une perte de 200 M$ ne représente qu'environ 0,3 % du chiffre d'affaires (environ 70 Md$ en 2017). Malgré l'importance de la somme en valeur absolue, on peut presque considérer ce sinistre comme attritionnel à l'échelle d'un grand groupe. À l'inverse, un *ransomware* qui coûte quelques milliers voire quelques dizaines de milliers d'euros à une petite entreprise sera considéré comme très sévère.

Ainsi la sévérité des sinistres cyber peut se calibrer selon une portion des revenus des victimes et bien que les données manquent encore, on s'attend à ce que la fonction de distribution du taux de destruction pour les petites entreprises soit plus sévère que celle des grandes.

Graphique 3
Exemple de calibration de la loi de sévérité des sinistres de type perte de données selon la taille de l'entreprise (chiffre d'affaires inférieur (S/M) ou supérieur (L/XL) à 100 M€)



Source : SCOR.

La fréquence

La fréquence est sans doute le paramètre le plus difficile à calibrer car, à part les informations publiques sur les pertes de données aux États-Unis (qui, encore une fois, n'estiment pas les pertes financières associées), les données de sinistres sont très peu nombreuses. Les sinistres attritionnels sont très majoritairement non déclarés.

On note malgré tout quelques caractéristiques de fréquence, notamment pour les grandes entreprises. Tout d'abord, il est assez commun

qu'un groupe de *hackers* cible un secteur d'activité en particulier. Les hôpitaux sont des cibles régulières, de même que le secteur de la grande distribution ou les institutions financières. De plus, une même entreprise est souvent victime de plusieurs attaques réussies et ces attaques se produisent à des moments où l'organisation est fragile (acquisition ou fusion en cours, par exemple). Enfin, les grands groupes très dépendants et très connectés à leurs sous-traitants, plus petits et moins bien protégés, peuvent être attaqués par ce biais.

Ces caractéristiques structurelles montrent que l'exposition des entreprises joue un rôle dans l'analyse des fréquences. Un mauvais score à cause d'une maturité faible et/ou d'une forte attractivité pour les attaquants va augmenter la fréquence des sinistres. On peut donc transposer le problème de l'analyse globale de la fréquence à celui de l'analyse du score d'exposition d'une entreprise ou, plus précisément, de l'écart du score par rapport à une valeur acceptable. Cette démarche s'inscrit bien dans le processus de souscription, mais dépend évidemment fortement de la qualité du calcul du score.

D'autres approches sont-elles possibles ?

Les attaques cyber sont conduites par des humains dont les motivations et les stratégies sont étudiées en détail depuis longtemps. Ils ont des objectifs de gain et ne lancent leur attaque que si elle peut leur rapporter suffisamment d'argent, de gloire ou de victoire idéologique. Dans cette logique économique, la théorie des jeux pourrait-elle être utilisée pour mieux estimer la fréquence des attaques ? Pourrait-elle apporter aux techniques actuarielles classiques un nouvel éclairage permettant de mieux appréhender ce risque ?

Quoi qu'il en soit et quelle que soit la modélisation choisie, la connaissance du risque, de ses mécanismes, des attaquants et des vulnérabilités qu'ils exploitent est indispensable. Peut-être plus encore que pour d'autres risques, la tarification du risque cyber d'une entreprise demande un fort degré d'expertise qui fait encore souvent défaut dans notre marché.

MODÉLISATION DU RISQUE DE CYBER-CATASTROPHE

L'économie numérique produit tous les ingrédients pour des cumuls de risque à grande ampleur

Les industries de réseaux et la dynamique de croissance exponentielle qu'elles produisent par leurs externalités se sont matérialisées tout au long du XX^{e} siècle, notamment dans le domaine du transport, de l'énergie ou des télécommunications. Pour autant, leur développement

et les situations de monopole qu'elles pouvaient générer se sont heurtés aux barrières physiques ou réglementaires dressées sur leur route.

L'avènement d'Internet et le développement des infrastructures permettant un accès étendu et performant à la toile semblent avoir repoussé les limites de l'effet de réseau. L'économie de la donnée se déploie avec des frictions minimes. Les échanges ne connaissent pas de frontières et les opérateurs, que ce soit dans le domaine des produits ou des services, créent des plateformes d'échanges entre clients de multiple nature dont la valeur croît avec la taille et qui peuvent toucher des milliards d'individus. En quelques décennies, les GAFAM (Google, Amazon, Facebook, Apple, Microsoft) ont détrôné les acteurs de l'ancienne économie au rang des plus fortes capitalisations boursières mondiales.

Cet effet de réseau, dicté par l'utilité et l'efficience, créé des concentrations extrêmes :

– Microsoft fournit presque 90 % des systèmes d'exploitation dans le monde ;

– Amazon Web Services est *leader* mondial en matière de services de *cloud* avec une part de marché de 35 % dans un marché mondial en très forte croissance (+48 % sur un an à la fin de 2018) et qui continue néanmoins à se concentrer ;

– Google a raflé la mise avec plus de 90 % des utilisateurs de moteurs de recherche ;

– sur le segment des smartphones, Apple et Google sont dans un duopole de fait pour les systèmes d'exploitation et les librairies d'applications mobiles ;

– en matière d'équipements de réseau, Cisco et Huawei fournissent plus des deux tiers des routeurs et Huawei (encore), Ericsson et Nokia équipent plus des trois quarts des infrastructures mobiles.

Nulle part ailleurs, la doctrine du *winner-takes-all* n'est mieux illustrée.

Standardisation des produits, concentration des services et connectivité à l'échelle mondiale sont les trois ingrédients d'une propagation et d'une accumulation de risque à grande échelle.

Des événements précurseurs

Si aucune cybercatastrophe d'ampleur n'est encore à déplorer, des événements récents révèlent la réalité du risque et informent sur sa capacité à se propager à grande échelle :

– WannaCry : ce logiciel malveillant de type rançongiciel se répand en mai 2017 à l'échelle mondiale. Il exploite une faille de sécurité (EternalBlue) présente dans certaines versions du système d'exploitation Windows. En quelques heures, plusieurs centaines de milliers

d'ordinateurs se trouvent contaminés dans plus de 150 pays. Leurs données sont chiffrées et inaccessibles. De grands groupes industriels sont affectés par des arrêts de production. Le coût économique de cette attaque a été estimé par plusieurs sources entre 4 Md$ et 8 Md$;

– NotPetya : cette autre attaque mondiale survient en juin 2017, un mois après WannaCry. Un logiciel de type *wiper* qui détruit les données exploite la même faille de sécurité que WannaCry, mais se répand de manière différente : il se propage à partir de l'Ukraine, utilisant une procédure de mise à jour d'un logiciel de comptabilité local. Là encore, plusieurs grandes entreprises mondiales se trouvent affectées par des disruptions importantes de leurs activités. La Maison Blanche en a attribué l'origine à la Russie et en a estimé l'impact économique à plus de 10 Md$.

Une modélisation du risque catastrophe en construction

Malgré un long historique de catastrophes naturelles, il a fallu attendre la fin des années 1980 pour voir émerger les premiers modèles de risques naturels et les désastres en Floride de l'ouragan Andrew en 1992 pour en faire une priorité du marché de l'assurance et de la réassurance. Les dommages économiques d'Andrew s'élevèrent à environ 26,5 Md$. Selon les méthodes d'évaluation alors en vigueur, le pire scénario catastrophe dans la région était évalué entre 7 M$ et 60 M$. Autant dire que personne ne croyait véritablement en ces chiffres.

Le risque cyber se trouve aujourd'hui dans une situation à peu près semblable à la période pré-Andrew pour les catastrophes naturelles, avec une différence de taille : il n'y a pas d'historique de catastrophes. Mais une autre différence tout aussi importante : c'est l'homme qui créé ce risque. Et enfin une exigence forte des parties prenantes (gestion de risque interne, régulateurs, agences de notation) pour parvenir à une maîtrise des expositions sans attendre que survienne le « Andrew » du cyber-risque. En bref, le marché cyber doit réaliser en quelques années ce qui a pris plusieurs décennies pour les risques naturels !

Les acteurs de marché sont donc engagés dans la construction de scénarios et de modèles en reprenant ce qui peut l'être des méthodologies existantes : construire des événements catastrophe plausibles ; identifier les paramètres d'exposition pertinents de l'assuré ; évaluer les dommages en fonction des vulnérabilités et calculer la perte financière pour l'assureur et le réassureur.

Cette démarche engagée depuis quelques années se fait pas à pas, en partant d'une approche déterministe par scénarios pour aller vers des modèles stochastiques de plus en plus sophistiqués.

L'approche par scénarios

Si l'homme est capable de la plus grande malveillance, son ingéniosité pour en prédire les manifestations n'est heureusement pas en reste !

Les agences de modélisation, les experts en cybersécurité et les souscripteurs cherchent donc à imaginer les événements (principalement des attaques, mais aussi des pannes informatiques) qui pourraient mener à des cyber-catastrophes d'ampleur pour le marché, tout en conservant des hypothèses plausibles. La probabilité de survenance est un facteur difficile à déterminer dans ce monde en perpétuelle évolution et sans historique significatif, mais c'est bien, en référence aux événements naturels, l'événement centenaire ou bicentenaire qui est recherché.

Les facteurs de corrélations sont assez faciles à identifier et tiennent aux trois caractéristiques de l'économie numérique citées plus haut :

– la standardisation des produits : une vulnérabilité logicielle exploitée par des attaquants peut induire des pertes (de données ou de production) chez une multitude d'assurés utilisant les mêmes équipements (logiciels ou matériels) ;

– la concentration des services : l'indisponibilité de services critiques comme le Cloud chez un prestataire majeur conduirait rapidement à une désorganisation voire à un arrêt des opérations chez ses nombreux clients ;

– la connectivité via le réseau : qu'il s'agisse du réseau interne à l'entreprise ou du réseau internet, elle est gage d'une propagation rapide et large des logiciels malveillants.

Le Lloyd's, par exemple, a publié et documenté un certain nombre de scénarios qui permettent d'évaluer la perte risque par risque et à l'échelle d'un portefeuille. Ces scénarios déterministes (ils représentent l'occurrence d'un événement défini) sont proposés chacun avec différentes variantes en termes de sévérité, auxquelles sont parfois assignées des périodes de retour.

Pour les appliquer, il faut disposer pour chaque police d'assurance des données d'exposition du risque (essentiellement le chiffre d'affaires et le secteur d'activité de l'assuré) et des termes du contrat (limite, franchise, garanties). Le calcul des dommages repose sur des éléments statistiques (part de marché de tel ou tel fournisseur de produits ou de services, probabilité et coût moyen de l'incident, etc.) et non sur les paramètres effectifs de chaque risque individuel.

Le tableau *infra* indique le coût économique global et le montant assuré ainsi calculé pour trois scénarios du Lloyd's dans leur variante la plus extrême.

Tableau
Trois scénarios de cyber-catastrophe

Nom du scénario	Description	Coût économique	Montant assuré
Mass vulnerability [9] (variante dite « extrême »)	Exploitation d'une vulnérabilité de type *zero-day* (sans correctif logiciel connu) présente sur un système d'exploitation largement utilisé qui résulte en une fuite massive de données chez les utilisateurs	28,7 Md$	2,1 Md$
Cloud down [10] (variante dite « *5.5-11 days* »)	Un fournisseur majeur de services Cloud aux États-Unis est victime d'un incident conduisant à une interruption prolongée des services à ses clients. Il en résulte une dégradation, voire un arrêt de leurs opérations qui dépendent de l'informatique	18,2 Md$	3,9 Md$
Bashe attack [11] (variante dite « X1 »)	Infection globale par un rançongiciel résultant en l'indisponibilité ou la perte de données et un arrêt prolongé des activités (attaque du type « WannaCry » ou « Notpetya »)	193 Md$	27 Md$

Source : Lloyd's projet Cyber Risk Management (CyRM).

Ces scénarios illustrent assez bien les facteurs de corrélation indiqués ci-dessus et les différents types de pertes assurées (réponse à incident, coûts de restauration des systèmes et données, notifications et réclamations à la suite de la fuite de données personnelles, perte d'exploitation directe ou consécutive au défaut d'un fournisseur, etc.).

Les montants ainsi calculés montrent une certaine variabilité et peuvent être discutés, mais ils suggèrent, alors que le taux de pénétration de l'assurance cyber est encore limité, que l'on fait face à des événements de taille potentiellement comparables aux catastrophes naturelles.

Vers une modélisation stochastique ?

Si l'approche déterministe donne une indication de l'exposition aux événements cyber sur certains scénarios spécifiques, elle ne permet pas d'établir une tarification du risque catastrophe, ni d'évaluer le besoin en capital pour porter ce risque.

Plusieurs agences de modélisation développent aujourd'hui des approches probabilistes. Certaines de ces entités sont déjà bien établies dans l'univers des risques naturels, d'autres se sont forgées récemment sur leur expertise en cybersécurité.

L'objectif est d'approfondir l'approche déterministe dans toutes les dimensions :

– créer des catalogues d'événements en modélisant probabilité et sévérité (profondeur et empreinte des dommages) ;

– affiner les nœuds de corrélation : identifier les acteurs majeurs pour les différents services critiques (*cloud*, fournisseurs d'accès à Internet, services de paiement, etc.), les logiciels et équipements clés (systèmes d'exploitation, bases de données, serveurs, etc.) ;

– identifier de façon plus précise les attributs de chaque assuré (quels fournisseurs ou quels logiciels utilisés ?) soit sur une base déclarative, soit par l'observation non intrusive des flux de trafic qu'ils génèrent sur Internet, c'est-à-dire leur empreinte numérique.

Comme pour les risques naturels, cette démarche permet de générer des distributions d'événements par occurrence et agrégées par année, aussi bien en matière d'impact matériel et financier pour les risques concernés (le taux de destruction) que de montant assuré et réassuré au travers des contrats en place. Les données en sortie, sous forme de tables d'événements ou de courbes de distributions, sont en tous points semblables à ce que produisent les modèles de catastrophes naturelles.

La difficulté de l'exercice tient évidemment à s'assurer que les catalogues d'événements soient bien représentatifs des scénarios redoutés, à la calibration des paramètres de fréquence et de sévérité et à l'établissement des modèles de coûts financiers. Il s'agit d'un travail prospectif tant la base de connaissance sur laquelle il s'appuie est encore bien limitée. Beaucoup reste encore à faire et comme pour les événements naturels, ces modèles devront être recalibrés à l'aune de l'expérience.

Un risque d'intensité à faible mutualisation

Si l'approche méthodologique présente des similitudes avec celle des catastrophes naturelles, des différences notables se font jour :

– la granularité est différente : la modélisation des événements naturels requiert une définition fine des caractéristiques structurelles et fonctionnelles de chaque bâtiment, ouvrage ou unité de production. Les modèles cyber s'intéressent eux à l'empreinte numérique de l'entreprise avec ses points d'entrées (adresses IP) et vont plutôt la regarder sous l'angle organisationnel avec ses filiales, ses activités et sa taille (chiffre d'affaires, nombre d'employés) ;

– l'intensité des événements est encore sujette à discussion, mais les modèles suggèrent des coûts économiques en dizaines de milliards de dollars, donc comparables aux risques naturels. Avec le développement des usages et une dépendance accrue vis-à-vis du numérique, avec surtout une pénétration croissante de la couverture des risques, il faut s'attendre dans les années qui viennent à des niveaux d'exposition de plus en plus élevés pour l'industrie de l'assurance et de la réassurance ;

– la diversité est ce qui fait le plus défaut aux risques cyber : contrairement aux tempêtes ou aux tremblements de terre, les événements cyber ne connaissent pas de limites, ni dans le temps, ni dans l'espace : on ne leur connaît pas de saisonnalité spécifique et ils peuvent se propager à l'échelle de la planète ;

– l'événement cyber est difficile à définir : contrairement aux périls naturels, il n'a donc pas de contours géographiques, son développement dans le temps peut être diffus et son attribution, donc son origine, est la plupart du temps impossible à déterminer avec certitude.

Faible diversité et forte intensité des catastrophes cyber créent une situation complexe pour le réassureur car il lui sera difficile de construire un équilibre par la mutualisation d'événements et, avec la croissance du marché, les besoins en capitaux risquent d'être rapidement élevés.

CONCLUSION : VERS UN SIGNAL PRIX DU RISQUE CYBER ?

L'adoption de plus en plus large des technologies numériques, dans les services comme dans la production industrielle, par les entreprises comme par les particuliers, est le mouvement de fond de la quatrième révolution industrielle.

Efficience et utilité semblent aujourd'hui les seuls critères d'achat ou d'usage de ces technologies. Et ceux-ci mènent à la concentration et la standardisation soulignées plus haut. Le directeur informatique s'équipera d'un parc matériel ou d'un logiciel harmonisé et de préférence chez les *leaders* de marché pour des raisons de coût et d'interopérabilité. L'externalisation auprès d'un petit nombre de fournisseurs de services Cloud devient la règle. La taille est aussi synonyme de performance et de pertinence pour les usagers du net : qu'il s'agisse de Google pour les recherches sur Internet, de Uber ou de Waze pour nos mobilités. D'autant plus que beaucoup de ces services sont gratuits. Selon l'adage, lorsque vous ne payez pas le produit, vous êtes le produit !

Bref, l'attitude des agents économiques conduit inéluctablement à la création de plateformes informationnelles gigantesques et à la perte de toute diversité sans que la sécurité ne soit pour autant garantie. Rien ne semble contrarier ce mouvement. Au-delà de quelques gesticulations géopolitiques, les États restent pour le moment bien silencieux face à ces géants qui contestent pourtant leur souveraineté.

Or ces attitudes d'achat ou d'usage conduisent, comme nous l'avons décrit dans ces lignes, à un risque cyber de plus en élevé, en fréquence comme en intensité. Les événements d'ampleur de ces dernières années,

qu'il s'agisse d'attaques ciblées ou à large spectre, ne portent pas encore le nom de risques majeurs ou de catastrophes bien qu'ils en aient les attributs.

Notre économie actuelle, qui repose sur le substrat numérique et la connectivité, ne pourra se développer sans couverture financière de ce risque.

La quantification du risque cyber par les assureurs et les réassureurs joue donc un rôle clé dans ce développement. Elle seule peut mettre en évidence le véritable prix du risque et les besoins en capitaux associés. Elle seule permet de révéler les contradictions entre prix d'achat et sécurité, entre efficacité et diversité.

Aidée par les réglementations de sécurité des infrastructures ou de protection des données qui se mettent en place, l'industrie de l'assurance en donnant un signal prix au risque cyber doit être un acteur majeur dans la transformation nécessaire de l'industrie numérique.

NOTES

1. Voir le site : https://www.lesechos.fr/2018/04/comment-les-fake-news-manipulent-les-marches-boursiers-988655 ; ou le site : https://www.lemonde.fr/economie-francaise/article/2016/11/23/comment-le-groupe-vinci-victime-d-un-hoax-a-chute-en-bourse_5036269_1656968.html.

2. Voir le site : https://en.wikipedia.org/wiki/Syrian_Electronic_Army.

3. Voir le site : https://en.wikipedia.org/wiki/Iranian_Cyber_Army.

4. Voir le site : https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

5. Un *ransomware*, rançongiciel en français, est un logiciel informatique malveillant prenant en otage les données. Le *ransomware* chiffre et bloque les fichiers contenus sur un ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer.

6. Voir le site : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf.

7. Voir le site : https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/.

8. Voir le site : http://fortune.com/2017/05/23/target-settlement-data-breach-lawsuits/.

9. Voir le site : https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report.

10. Voir le site : https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down.

11. Voir le site : https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack.