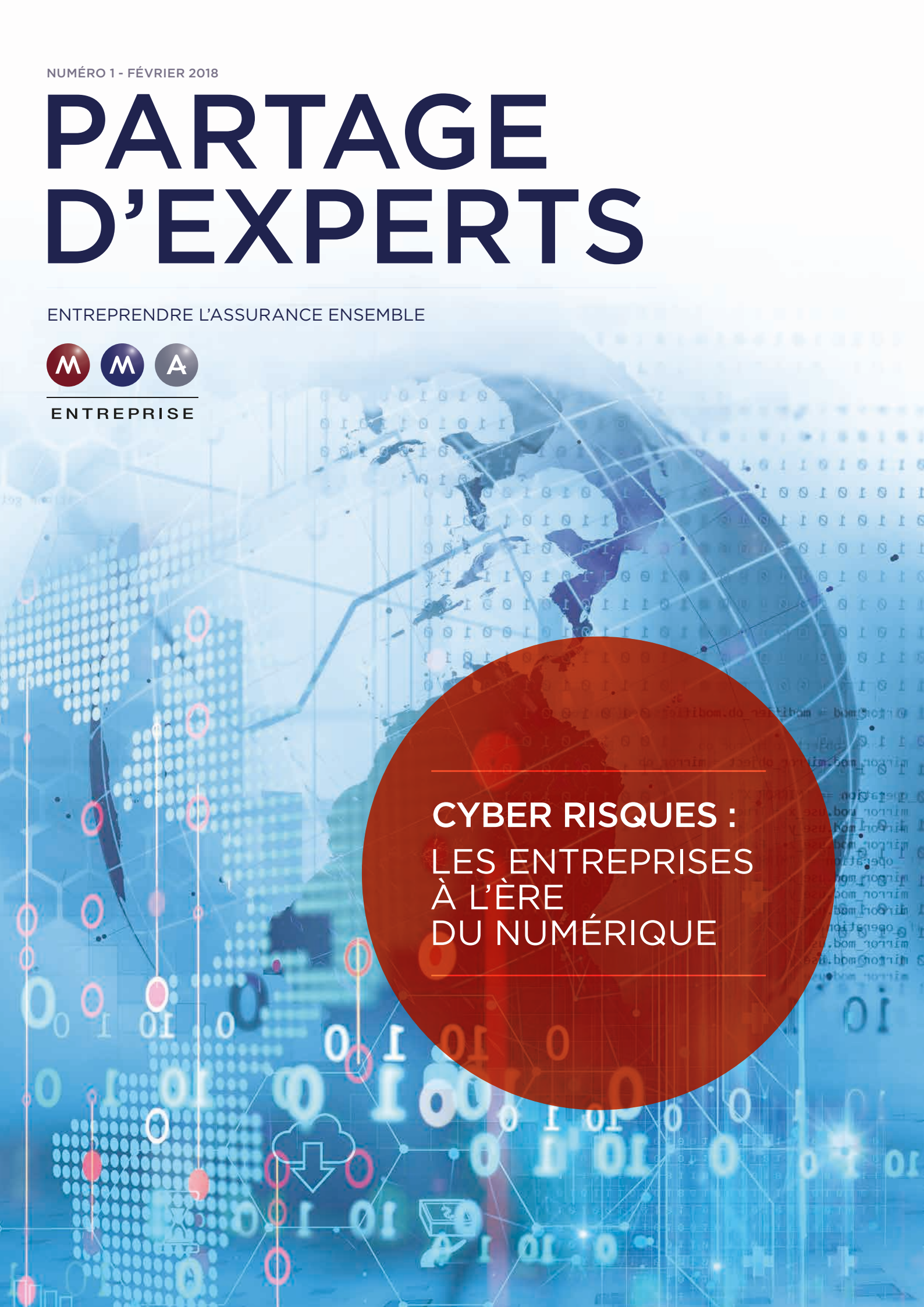
NUMÉRO 1 - FÉVRIER 2018

PARTAGE D'EXPERTS

ENTREPRENDRE L'ASSURANCE ENSEMBLE

MMA ENTREPRISE



CYBER RISQUES :
LES ENTREPRISES À L'ÈRE DU NUMÉRIQUE

SOMMAIRE

Numéro 1 – Dépôt légal : Février 2018 – Direction de la publication : Olivier Jarry – Direction de la rédaction : Dominique Orain – Comité de rédaction : Michel Hornacek, Odile Lasternas Brécy, Valérie Leguay-Rondeau – Document publicitaire à caractère non contractuel – Éditeur : MMA IARD – Société anonyme - Siège social : 14, boulevard Marie et Alexandre Oyon, 72030 Le Mans Cedex 9 – Conception/réalisation : EXIRYS – Imprimerie MMA Le Mans – Crédits photos : Ekaphon Maneechot, Gary Killian, Artens, ImageFlow, monsitj, Pix'HEL, Benoît Granier, Laetitia Duarte – N° ISSN : En cours. Documentation réservée à l'information des courtiers partenaires MMA Entreprise.

ÉDITO

Olivier JARRY
Directeur Central Entreprises MMA

« Notre ambition commune est d'accompagner les entreprises dans la gestion dynamique de leurs risques. En tant que professionnels de l'assurance, nous observons les évolutions sociétales, nous analysons notre environnement, nous recherchons de l'information et des données, nous développons des solutions.

Échanger avec l'ensemble des acteurs qui sont au cœur des problématiques d'aujourd'hui et de demain nous amène à parfaire notre compréhension pour anticiper et mieux maîtriser les enjeux auxquels les entreprises doivent faire face. C'est ce que nous voulons explorer avec vous dans ce nouveau magazine.

Le monde est digital. Tous les secteurs sont impactés. De nombreux métiers sont ou seront profondément transformés par cette nouvelle réalité qui abolit les frontières.

Le cyber espace constitue une dimension supplémentaire dans laquelle les entreprises évoluent. Il induit de nouveaux risques bien souvent immatériels et encore trop souvent sous-estimés. Dans ce nouvel environnement, qui peut encore considérer que le traitement des risques cyber ne constitue pas un volet majeur de la protection des entreprises ?

Dans ce premier numéro de « Partage d'Experts », nous souhaitons partager avec vous les réflexions et connaissances d'experts qui nous accompagnent sur ces sujets. »

SCOPE

Le coût des cyberattaques en France est évalué en 2016 à

1,5 Milliard

d'euros*

“ Dans une certaine forme, la **cyberguerre** a commencé. Quand des attaques peuvent détruire les moyens de production d'une entreprise, les services administratifs d'un État ou les bloquer pendant quelques jours, si ce n'est pas une guerre, qu'est-ce que c'est ? ”

4 165

cyberattaques ont été détectées en France en 2016**

*Sources : *Alain Juillet, **Étude The Global State of Information Security® Survey 2017*

5 QUESTIONS À ...

Alain Juillet a été un des hauts responsables du contre-espionnage français au sein du SDECE, l'ancêtre de la DGSE. Il a aussi été dirigeant d'entreprises : *Ricard, Suchard-Tobler, l'Union laitière normande, Bongrain, France Champignon.* Il intervient à l'ÉNA et à l'École Nationale de la Magistrature.

ALAIN JUILLET

Alain Juillet est le président de l'Académie d'Intelligence Économique, créée en 1993. Elle favorise les réflexions et les échanges entre entrepreneurs, chercheurs, experts, étudiants, dirigeants, journalistes, etc. sur l'évolution des technologies et des techniques.

Comment analysez-vous les cyberattaques mondiales de mai et juin 2017 ?

Elles auraient pu être évitées. Elles ont exploité des failles informatiques pour lesquelles Microsoft avait donné les clés pour les rendre inopérantes dès février-mars. Nous vivons dans un cyberespace où tout va beaucoup plus vite que dans le monde auquel nous étions habitués. L'anticipation est un enjeu majeur dans la cybersécurité.

Que préconisez-vous ?

Un changement d'état d'esprit est nécessaire. Il faut regarder la réalité en face. Tous les paramètres changent. Nous avons beaucoup investi pour améliorer l'efficacité de nos systèmes et les capacités de veille et de surveillance mais, ces dix dernières années, la cybersécurité a été le parent pauvre du cyberespace. En cas d'attaque, une organisation doit être capable de la parer. Sinon, il faut prendre immédiatement les mesures nécessaires. Nous sommes encore trop dans la réaction alors que nous devrions anticiper. C'est d'autant plus regrettable que nous avons d'excellents spécialistes en France.

Que visent ces attaques ?

Tous les secteurs économiques sont visés. Trois aspects sont à prendre en considération :

- L'intérêt des États, c'est-à-dire les intrusions et les interceptions des grands pays comme les États-Unis, la Chine, la Russie ; il s'agit d'aller chercher des informations ou de déstabiliser pour conforter une politique d'État.

- Ensuite, vous avez les entreprises dont certaines sont malintentionnées. Les Américains parlent des « Rogue Companies », des entreprises voyous qui n'hésitent pas à payer des hackers pour collecter des renseignements sur tout ce qui peut les aider : la recherche, l'organisation industrielle, les fichiers clients... pour améliorer leurs performances ou battre des concurrents.

- Enfin, il y a les groupes criminels qui pillent des informations dans des entreprises pour les revendre à d'autres, ou pour les utiliser dans le cadre d'un commerce illicite.

Comment agissons-nous face à ces menaces ?

La France a pris le taureau par les cornes en créant l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information. Nous sommes dans une situation nettement meilleure que la plupart des pays d'Europe. Nous avons déployé des efforts en matière d'innovation et de recherche, et développé des incubateurs et des startups. Malheureusement, la France est le pays des silos ; la transversalité n'est pas dans notre culture.

Peu d'entreprises réussissent à faire travailler en commun différentes fonctions ou différents départements. La prise de conscience des dirigeants progresse, mais elle reste lente.

Que faire ?

Ce que fait l'ANSSI est formidable, mais elle ne regroupe que 500/600 fonctionnaires. C'est insuffisant pour traiter les problèmes de 3 millions d'entreprises.

Il faut donc des relais efficaces au niveau des fédérations, des organisations et des syndicats professionnels dans tous les secteurs de l'économie.

SCAN

900 M€
montant estimé des rançons récupérées par les hackers en 2016*

2600
cybercombattants numériques d'ici à 2019 en France**

22%
d'entreprises victimes de ransonware en 2016***

« La sécurité ne doit pas bloquer l'innovation, le progrès, la productivité et le développement. Il faut cybersécuriser nativement, mettre en œuvre une chaîne de confiance de bout en bout »

Jean-Marie LETORT,
Vice-président Stratégie Activité Cybersécurité de Thales.

*Sources : *Conférence «Confiance» de l'Institut Esprit Service au Medef le 20 avril 2017, **Alain Juillet, ***Baromètre Euler Hermes Mai 2017*

LES ENTREPRISES À L'ÈRE DU NUMÉRIQUE

LE NOUVEAU VISAGE DE LA CYBERCRIMINALITÉ

Au centre de la réflexion stratégique autour du numérique, la sécurité représente un défi majeur pour les entreprises. Comment l'intégrer dans les processus sans freiner l'innovation ? La question agite l'ensemble des acteurs mondiaux, à tous les niveaux et dans toutes les strates de la société. Explications.

Deux cyberattaques sans précédent en mai et en juin 2017, Wannacry et Petya, ont ciblé des centaines de milliers d'ordinateurs dans le monde entier, essentiellement en Europe. Elles confirment l'ampleur des enjeux numériques auxquels sont confrontées les institutions, les organisations et les entreprises.

CYBERATTAQUES...

Certes, la mutation technologique est un formidable créateur de valeur ajoutée et un accélérateur d'innovation dans tous les secteurs, économique, social et sociétal. Mais cette révolution n'est pas sans danger. Ransomware[1], hacking, insécurité des données personnelles et corporate...

« Nous sommes déjà dans la cyberguerre, explique Alain Juillet, Président de l'Académie d'Intelligence Économique (Lire son interview p. 4 et 5). Elle vise des produits, des services, des systèmes informatiques et le Big Data. Or, si l'on retire le cœur d'activité d'une entreprise, il ne lui reste rien ».
On se souvient notamment de Domino's Pizza aux États-Unis, victime d'un vol de 15 millions de données client revendues ensuite à une entreprise concurrente.

... ET SÉCURITÉ

Le business de la cybercriminalité est en pleine croissance... et aujourd'hui, il se démocratise ! « Il ne s'agit plus seulement d'une délinquance de haut niveau », s'inquiète Nicolas Arpagian, directeur Stratégie Orange Cyberdéfense. « Il est désormais très facile de devenir un "petit hacker" en prenant quelques "leçons" sur Internet ». Résultat ? En France, pas moins de 3 millions d'entreprises, représentant plus de 99% du tissu économique hexagonal, sont ainsi des proies potentielles...
Dominique Jeune, manager des Risques techniques de MMA, qui développe des offres d'assurance face aux cyber risques en France, note d'ailleurs qu'en 2016 : « 75% de la sinistralité sont des faits d'extorsion ».

GÉRER LA CRISE... AVANT QU'ELLE NE SURVIENNE

Il n'y a pas de bouclier magique pour se prémunir ! Les modes opératoires évoluent si vite qu'il est utopique d'échapper aux agressions informatiques. « D'où l'importance de mettre en place des plans d'actions efficaces, de travailler sur la culture de la réactivité », insiste Nicolas Arpagian. En d'autres termes, les entreprises qui réagiront le plus vite sont celles qui auront anticipé les menaces par une stratégie de gestion de crise. « Il faut identifier l'attaque le plus vite possible, la circonscrire, la neutraliser et trouver des solutions adaptées à un retour à la normale ».

Une vision largement partagée par Dominique Jeune : « Dans nos contrats cyber, nous prévoyons un volet d'assistance. En collaboration avec des prestataires sélectionnés en fonction du problème, nous remettons les choses en ordre puis nous couvrons le sinistre ». Une expertise et un accompagnement de plus en plus recherchés par les entreprises.

> *" Les entreprises qui réagiront le plus vite sont celles qui auront anticipé. "*

[1]Piratage informatique contre une rançon. Littéralement veut dire : « rançongiciel ».

COUVRIR LES CYBER RISQUES AU-DELÀ DES PROBLÉMATIQUES INFORMATIQUES

Dominique JEUNE, manager des Risques techniques de MMA

Les solutions d'assurances pour les risques informatiques sont connues depuis longtemps, réparties dans plusieurs polices : tous risques informatiques, fraude informatique, dommages aux biens, jusqu'à la protection juridique pour l'e-réputation.

Le marché américain est le premier à avoir fait émerger des garanties spécifiques cyber, qui s'appliquent aux conséquences d'atteintes aux données informatiques, en l'absence de dommage matériel.

Avec l'arrivée d'assureurs américains sur le marché européen et une volonté de développement rapide des acteurs locaux, le segment des assurances cyber est immédiatement apparu comme extrêmement concurrentiel. En s'appuyant sur des définitions existantes ou des référentiels partagés, les garanties proposées par les acteurs de la place sont souvent similaires.

La différence essentielle repose sur le type d'évènements couverts. « MMA a fait le choix de concevoir une offre complète et innovante qui se structure selon les besoins du client. Au-delà des actions de piratage et actes malveillants, nous couvrons les erreurs humaines de manipulation et les dysfonctionnements informatiques ». Un bouclier déterminant pour les entreprises en plus, bien sûr, des plans de sauvegarde des données et de l'éducation des utilisateurs aux bonnes pratiques.

Les portefeuilles clients commencent à s'étoffer, et avec près de 20 000 assurés, MMA acquiert une expérience significative sur la sinistralité de ce risque. Du fait que le marché européen n'ait pas enregistré à ce jour de sinistre majeur, une vive concurrence s'installe sur les tarifs pratiqués. Pour autant, les prix attractifs ne suffisent pas à déclencher une souscription massive de polices cyber.

Il reste donc à convaincre les entreprises, qui ne sont pas toutes sensibilisées à ces problématiques et ne perçoivent pas le risque pour leur activité. « Les dirigeants d'entreprise doivent réaliser qu'il ne s'agit pas d'une garantie gadget, d'une garantie accessoire mais que les cyber risques sont devenus un enjeu majeur pour l'entreprise ».

“ L'assurance cyber risque représente un bouclier déterminant pour les entreprises. ”

CYBER RISQUES : LE SERVICE AVANT L'INDEMNISATION FINANCIÈRE

Bertrand Pelletier, responsable du domaine Indemnisation Courtage DAB-RC-RT chez MMA

Les attaques des systèmes informatiques peuvent se révéler particulièrement dévastatrices en un temps record. De la rapidité de la réaction dépend donc en grande partie l'importance des dommages.

« D'autant que les attaques sont portées généralement le week-end, lorsque la veille de sécurité informatique est la moins présente, majoritairement depuis l'étranger, ce qui complique leur traçabilité », souligne Bertrand Pelletier, responsable du domaine indemnisation courtage de MMA. Aujourd'hui, les cybercriminels opèrent majoritairement par des actions de piratage de données de masse, sans réel ciblage. Pour autant, dès lors que les données stratégiques de l'entreprise sont touchées, se pose aussi la question de la confidentialité. La relation entre l'assureur et le partenaire en charge de rétablir le système doit être transparente.

« Notre position est de favoriser l'intervention du prestataire habituel de l'entreprise. À défaut, nous établissons un accord de confidentialité strict ». En cyber risques, il s'agit peut-être plus d'apporter un service de qualité que de transmettre simplement une indemnisation financière, même si cette dernière est évidemment importante.

« Notre prochain défi sera certainement de réagir avec autant de réactivité en cas de sinistres concernant les objets interconnectés. On peut prendre à cet égard l'exemple des milliards de machines, reliées entre elles, qui pourraient, à la suite d'une cyberattaque, entraîner un risque majeur d'arrêt complet de la production ou de dommages matériels à grande échelle ».

ASSURER, C'EST AVANT TOUT ANTICIPER

Éric Lagarde, directeur des Offres entreprises de MMA

Face à une cyberattaque, les entreprises sont confrontées à de multiples problématiques : arrêt d'activité, perte ou altération des données clés…

En complément de l'offre cyber, bénéficier d'un contrat gestion de crise permet aux entreprises d'être accompagnées en amont dans une démarche de prévention et de compréhension de leurs risques. L'anticipation est fondamentale pour limiter les effets d'un sinistre, voire même l'éviter.

« Pour réagir de la façon la plus efficace possible, il faut avoir parfaitement évalué le risque, disposer d'un réseau d'experts et avoir mis en place des processus de gestion de crise précis », explique Éric Lagarde, directeur des Offres entreprises chez MMA.
Une véritable (r)évolution du métier d'assureur : « Nous sommes désormais partenaires et plus seulement indemnisateurs ».

Selon le profil et la taille des sociétés assurées, un diagnostic de vulnérabilité préalable est effectué pour établir un plan d'anticipation en cas de survenance d'une crise, document essentiel à la prévention et la gestion du risque. Si le sinistre advient, « nous jouons notre rôle d'assureur-indemnisateur, puis nous reprenons notre casquette de partenaire pour aider l'entreprise à relancer son activité au plus vite. Un soutien complémentaire et inestimable pour les entreprises face aux cyber risques, dont les effets sont encore trop souvent sous-estimés. »

Obligation d'informer ses clients en 2018

La mise en application des règlementations européennes définies fin 2015, visant à protéger le consommateur, renforce les obligations des entreprises en matière de données.

À partir du 25 mai 2018, avec la mise en application du nouveau règlement européen sur la protection des données (RGPD) les entreprises devront déclarer à la CNIL toute violation de données et informer leurs clients en cas de détournement de celles-ci. Une obligation déjà en vigueur pour des administrations telles que la Défense, qui sera donc étendue à toutes les sociétés.

En cas de manquement, les sanctions iront de l'avertissement à l'application d'une amende qui pourra atteindre plusieurs millions d'euros.

MMA couvrira les frais de notification engendrés pour avertir les clients dont les données auront pu être détournées. En revanche, si l'entreprise recevait une amende de la CNIL pour non-respect de l'obligation de déclaration, conformément aux dispositions légales, ces frais ne pourraient pas être pris en charge.

SPHÈRE

Le numérique s'est imposé dans notre environnement. Tous les secteurs, toutes les filières et tous les publics sont impactés. S'il existe des différences de maturité, d'usages ou de technologies, la numérisation est un élément déterminant dans l'évolution de nos sociétés. Menaces ou opportunités pour les acteurs économiques, le digital est au coeur des sujets stratégiques. Une prise de conscience des enjeux est cruciale pour les décennies à venir. Jérôme WALLUT partage sa vision.

LE NUMÉRIQUE EST NOTRE ENVIRONNEMENT

Quelle est la place du numérique dans le monde ?

Le numérique est devenu notre environnement, il touche à tout et nous concerne tous. La différence ne réside pas dans la qualité des applications. Amazon et Google sont quasiment identiques aux États-Unis et en France. Tout se joue aujourd'hui sur la qualité des réseaux et sur les nouveaux usages.

La Corée du Sud est sans doute le pays le plus avancé sur ces deux points. Elle commence à utiliser la 5G qui équivaut à la 4G multipliée par 100 ! La vitesse et la nature des données que vous pouvez échanger sont considérables. Vous ne vous posez plus la question des réseaux. En France, nous avons encore des zones blanches[1].

Peut-on parler de pratiques différentes ?

Il y a des différences de culture. Des applications peuvent être influencées par leurs inventeurs mais les usages sont quasiment identiques partout. Dans tous les pays, les publics ont pris conscience de leur pouvoir.

En Chine par exemple, la gestion de son réseau personnel fait partie de l'ADN. Sur les sites internet, il y a des espaces de conversations. Certes, ils sont encadrés mais, pour le reste, les internautes ont pris le pouvoir.

Qu'attendent les utilisateurs ?

En 2008, le génie de Steve Jobs n'a pas été d'inventer le smartphone mais l'App Store et le concept de Software Development Kit (SDK), invitant les développeurs du monde à créer autant d'usages qu'ils veulent.

Tous les secteurs d'activité s'engagent, y compris dans le domaine des assurances avec Limonede (une assurance en peer to peer développée dans la Silicon Walid près de Tel Aviv) ou Wilov (une assurance automobile selon l'usage du véhicule) pour ne citer qu'eux.

Les App Store, ce sont 2,5 millions d'applications et 70 milliards de téléchargements. Mais, 70% des applications sont utilisés moins de 3 fois, ou téléchargés moins de 100 fois.

En clair, nous sortons de l'hystérie de consommation. La nouveauté qu'on trouvait géniale, brièvement, ne nous amuse plus. Désormais, nous choisissons des usages pour l'expérience qu'ils procurent.

JÉRÔME WALLUT

Jérôme WALLUT est un spécialiste du digital et de ses applications. Après avoir co-fondé en 1997 Connectworld, filiale digitale du groupe Havas, puis Human to Human en 2003, et jusqu'en 2012, il prend en charge le digital de W&Cie. Aujourd'hui, il est associé chez ICP Consulting et fondateur de WOUS. Il enseigne à Sciences-Po Paris.

Les plateformes ne remplacent-elles pas les relations humaines ?

On pense à son assureur lorsqu'on a un sinistre. À l'instar de nombreuses professions réglementées (notaires, huissiers, experts comptables), les assureurs, qui sont aussi des tiers de confiance, ont un rôle de conseil essentiel à jouer.

Cette fonction ne sera pas prise en charge par les machines mais s'ils laissent faire, les plateformes intermédieront leur métier. D'ici à 20 ans, les métiers et les entreprises seront fondés sur le conseil, la proximité et la confiance, sur la partie de ce que les technologies et les automatismes ne pourront pas fournir. L'humain fera toujours confiance à l'humain.

[1]Zone blanche : territoire qui n'est pas desservi par un réseau donné, de téléphonie ou Internet.

61,4%
des utilisateurs
de smartphones en France
seraient **géolocalisables**

Source : IBM

Vous disiez que les internautes ont pris conscience de leur pouvoir. Qu'est-ce que cela implique ?

La data a de la valeur et est une valeur. La question de fond porte sur le don des datas et ses contre-parties : elle concerne celui qui donne les datas, celui qui les reçoit et celui qui les utilise. Que font Google et les autres des données qu'on leur transmet ? Depuis plus de 20 ans, nous donnons nos datas, sans nous poser de question, parce que nous sommes ravis de profiter de tous les produits et services de Google et Amazon.

Les lobbyistes de Google occupent un immeuble entier à Bruxelles et ont pour objectif d'empêcher la Commission européenne de prendre des positions défavorables à leur encontre.

Les règlementations ne suffiront pas. Il faut imposer aux GAFA[2] de nous expliquer en quoi et comment ils les utilisent et, éventuellement, le contre don que l'on en tire. Nous devons passer de l'injonction à la conversation mature. C'est l'éthique qui générera du règlementaire et pas le contraire. Les États-Unis ne seront pas à l'origine d'une vision citoyenne de la data mais probablement l'Europe parce que notre sensibilité à ces questions est plus forte.

[2]Géants du web : Google, Apple, Facebook, Amazon

EN SAVOIR **PLUS**

Jérôme WALLUT est l'auteur de ***« Patrons n'ayez pas peur ! »*** paru aux éditions Cent Mille Milliards.

Comment engager une démarche de transformation de son activité quand on ne maîtrise pas tous les éléments d'une mutation aussi gigantesque que celle engendrée par le digital ? Ce livre déconstruit les idées reçues qui freinent un processus pourtant à l'oeuvre depuis plus de dix ans dans les entreprises.

Notre ambition avec les courtiers **Entreprendre l'assurance ensemble**

MMA est un expert du risque d'entreprise.
Nos spécialistes en cyber
vous apportent des solutions sur-mesure
avec des garanties complètes
pour protéger les entreprises
des conséquences d'une cyberattaque.
À vos côtés, nous anticipons et couvrons
l'évolution des risques de vos clients.

MMA
ENTREPRISE