www.pwc.fr

Le marché de la cyber-assurance : la révolution commence maintenant

Janvier 2016

pwc

Le cyber risque devient central pour nos économies. La cyber-assurance pourrait constituer une protection efficace contre la cybercriminalité. Cependant, le marché peine à décoller car de nombreux défis restent à surmonter. Malgré certains obstacles, plusieurs facteurs promettent un bel avenir à la cyber-assurance. Nous estimons que la cyber-assurance est un marché stratégique pour les assureurs. Il est d'ores et déjà possible de distinguer les caractéristiques des futurs leaders de la cyber-assurance.
Pour évaluer la situation actuelle et le potentiel du marché de la cyber-assurance, la présente publication analyse en partie les résultats d'une étude menée conjointement par PwC et l'IFOP datant de septembre 2015.

Pauline Adam-Kalfon
Directrice Assurance
PwC Consulting
Pauline.adam-kalfon@fr.pwc.com
https://fr.linkedin.com/in/paulineadamkalfon

Guy-Philippe Goldstein
Senior Analyst - Cyber-Desk, Wikistrat
Contributeur sur les questions de cyberdéfense à la revue académique de l'INSS (Institute for National Security Studies, Tel-Aviv)
https://fr.linkedin.com/in/guyphilippegoldstein

01

Pourquoi le risque « Cyber » devient central pour nos économies ?

Des attaques qui ne cessent d'augmenter

Au cours des deux dernières décennies, la fréquence et la gravité des incidents dont l'origine se situe dans les systèmes informatiques n'ont fait qu'augmenter. Les erreurs de logiciels, dont le coût global est très difficile à évaluer aujourd'hui, et qui pourraient peser au moins plusieurs centaines de milliards de dollars annuels au niveau mondial, impactent toutes les industries - de la finance de marché, frappée en 2010 par un crash boursier lié à des comportements non expliqués des automates de trading, aux multiples erreurs involontaires dans les logiciels de voitures.

Rien qu'en 2014, 65 000 voitures Ford Fusion ont été rappelées en Chine pour risques de redémarrage automatique inopiné 30 minutes après stationnement sous certaines conditions ; 102 000 Audi A4 Sedan en raison de risques logiciels qui désactiveraient l'airbag ; et 175 000 Honda Fit au Japon en raison de risques logiciels pouvant donner lieu à des accélérations ou décélérations incontrôlées du moteur.

L'exploitation malveillante de ces vulnérabilités est en progression constante : le nombre de cyber-attaques recensées a progressé de 38 % dans le monde en 2015 – et de 51 % en France. Cette menace constitue un coût aujourd'hui évalué au niveau mondial à environ 400 milliards de dollars. Pour les États-Unis d'Amérique, l'Union Européenne ou la Chine, le coût de la cyber-criminalité représente autour de 0,5 % de leurs PNB respectifs. À titre de comparaison, cela représente environ la moitié de l'économie mondiale du trafic illicite de drogue. Les réseaux criminels qui exploitent ces failles sont en train de réorganiser leurs activités. Ainsi, une translation de la délinquance physique est-elle en train de s'opérer vers la « cyber-délinquance ». Aux États-Unis, le nombre de braquages de banques a été réduit de 90 % en dix ans : pourquoi prendre des risques vitaux, lorsque le piratage organisé de plus d'une centaine de banques sur trente pays peut rapporter jusqu'à un milliard de dollars, comme révélé en février 2015 ? Cette évolution est favorisée par la faible capacité de recours et de poursuite judiciaire pour les entreprises. Cette nouvelle criminalité, toujours plus sophistiquée, parvient, à l'image d'un organisme parasite, à s'adapter plus vite que son « hôte », en même temps que ce dernier augmente ses défenses. Dans cette dialectique entre l'épée et le bouclier existe une asymétrie, qui donne plutôt l'avantage à l'attaque. Cette criminalité reprend aussi les codes commerciaux que l'on retrouve sur le net : les outils de cyber-criminalité sont de plus en plus simplifiés, distribués largement sur le dark web et parfois même avec des garanties de remboursement en cas de mauvais fonctionnement. On peut parler de l'émergence de plateformes de « Crime-as-a-Service », qui font écho aux plateformes de « Software-as-a-service » distribuées sur le cloud.

Ce « marché » repose sur la coopération en réseaux des différents acteurs criminels : des multiples spécialistes techniques jusqu'à leurs financiers. Il est par ailleurs entretenu par des vulnérabilités nouvelles qui apparaissent tous les jours alors que les infrastructures ne peuvent être mises à jour quotidiennement et que la surveillance des entreprises est largement défaillante et sous équipée. Le risque résiduel des entreprises ne sera jamais nul.

Dès lors, il devient de plus en plus essentiel pour les entreprises de réinvestir dans la cyber-sécurité et d'instaurer avec plus de rigueur des dispositifs de contrôle et de surveillance. Et l'on constate d'ailleurs que les budgets de cyber-sécurité des entreprises ont augmenté au niveau mondial en 2015 ; le marché mondial de la cyber-sécurité se développe rapidement – il représente aujourd'hui environ 77 milliards de dollars et devrait atteindre entre 130 et 170 milliards de dollars d'ici 2020.

D'autant que ce sont les systèmes industriels qui sont désormais menacés. Selon le Bundesamt für Sicherheit in der Informationstechnik (BSI), à la fin de l'année 2014, une aciérie en Allemagne a vu ses systèmes de contrôle piratés informatiquement via un maliciel simplement envoyé par email. Les hauts fourneaux de cette aciérie n'auraient pu être arrêtés, provoquant des dommages très significatifs. Dans le courant de l'année 2014, un maliciel baptisé « Havex » a été identifié, capable d'espionner et de comprendre le fonctionnement de systèmes SCADA de plusieurs groupes industriels européens, en particulier dans l'énergie.

Ces systèmes SCADA (Supervisory, Control and Data Acquisition) utilisés pour le contrôle et le pilotage des infrastructures industrielles, deviennent particulièrement vulnérables aux cybers attaques. Leur protection par l'isolation physique ou le fonctionnement manuel se réduit rapidement, en raison de leur connexion aux réseaux IT et à Internet. De plus, les protocoles propriétaires ne constituent plus des barrières défensives. Enfin, pour des raisons de legacy, les acteurs concernés utilisent encore des systèmes obsolètes, dont les vulnérabilités sont connues et facilement exploitables.

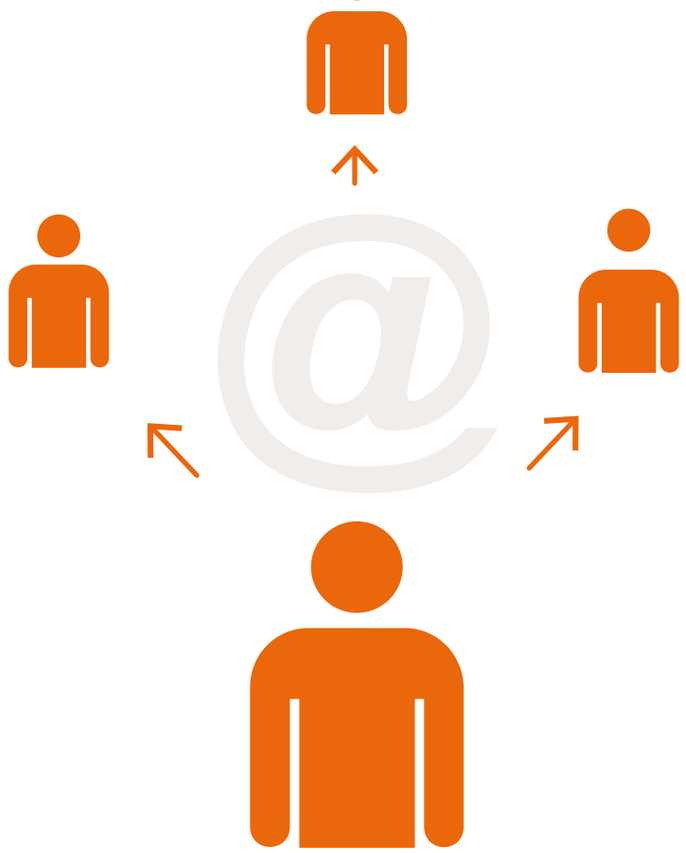
Une escalade qualitative des attaques

Cette augmentation du nombre d'incidents s'accompagne d'une évolution « qualitative » des attaques et de leurs coûts. Le nombre de vulnérabilités informatiques – les failles exploitables par des acteurs malveillants – continue d'augmenter de manière significative : plus du quart de toutes les vulnérabilités informatiques jamais recensées par le registre du National Institute of Standards & Technology aux États-Unis sont apparues au cours des 36 derniers mois. Ces vulnérabilités se retrouvent désormais dans toutes sortes de systèmes. En décembre 2014, les systèmes de contrôle industriel d'une aciérie en Allemagne ont été piratés via la réception d'emails. En mai 2015, la FAA envoyait une circulaire d'urgence demandant une réinitialisation tous les 248 jours de certains systèmes informatiques sur les Boeing 787. Deux mois plus tard, des hackers éthiques ont pu prendre le contrôle à distance d'une jeep Cheerokee, forçant Chrysler à demander un contrôle technique de plus de 1,4 millions de véhicules.

Mais surtout des conséquences humaines

Ces risques, désormais très concrets, ont un coût financier qui finit par peser sur les directions des entreprises et des institutions. L'administration fédérale de l'Office of Professional Management (OPM) devra probablement débourser plus de 330 millions de dollars suite à la fuite de données dont elle a été victime entre mars 2014 et avril 2015. Si le coût de la fuite de données pour la société Target en décembre 2013 a pu se limiter à 105 millions de dollars après couverture des assurances et défiscalisation des pertes, l'attaque a néanmoins coûté son poste au DSI et a pesé sur la décision de départ de son CEO. La fuite des données dont ont été victimes Sony Pictures Entertainment ou Avid Life Media (Ashley Madison) a pesé sur l'éviction de leurs dirigeants. Les conseils d'administration évaluent désormais le risque « cyber » de manière très fréquente – une étude de 2015 du NYSE note que sur un échantillon de 200 entreprises cotées, 4/5e des conseils d'administrations discutent de questions de cyber-sécurité soit systématiquement à chaque réunion, soit à la plupart des réunions.

Pour autant, ce risque demeure mal maîtrisé. Dans cette même étude, près de 2/3 des conseils d'administration interrogés considèrent qu'ils n'ont pas confiance dans la protection de leur entreprise en termes de risque « cyber ». L'évolution rapide de l'environnement digital ne va qu'amplifier ces risques et les craintes qui y sont liées. L'essor en cours de l'internet des objets et de la robotisation « de masse » des services est une formidable source d'optimisation via l'analyse des données ou la gestion automatisée des processus. Mais cette accélération de la numérisation pourrait également multiplier jusqu'à 5 le coût des incidents cybercriminels et les porter au niveau mondial à 2000 milliards de dollars d'ici à peine 5 ans. Le risque « cyber » pourrait devenir rapidement incontournable.



02

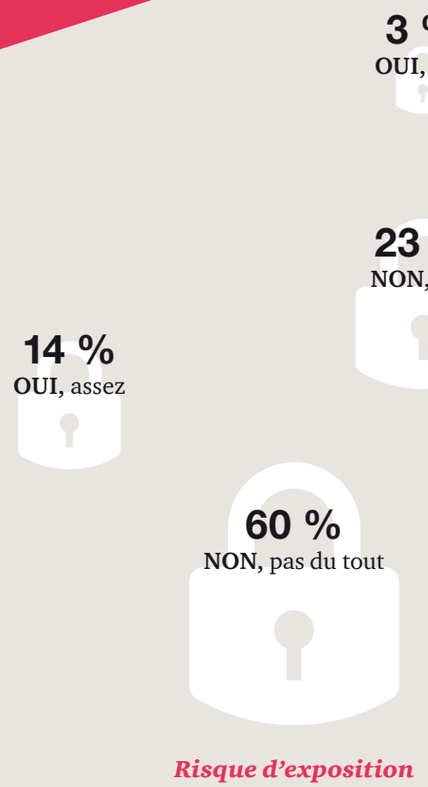
La Cyber-assurance : un nouveau marché encore limité à très haut potentiel

Une demande de cyber-assurance limitée mais à haut potentiel

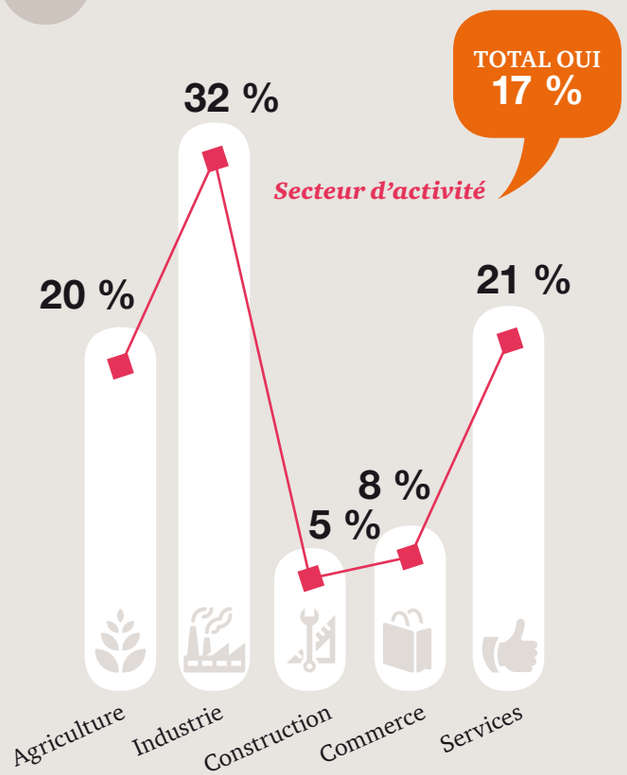
Comme tout marché de nouveaux services, celui de la cyber-assurance devrait bénéficier d'une prise de conscience rapide et d'effets viraux. Pourtant, aux États-Unis, là où le marché semble le plus développé, il n'était que de 2,4 milliards de dollars en 2014 – l'Europe continentale ne constituant qu'une fraction très mineure de ces montants. La couverture du risque ne concernerait que 6 % des entreprises aux États-Unis (d'après étude Biener et al.). En Grande Bretagne, seules 2 % des grandes entreprises seraient couvertes de manière explicite contre le risque « cyber » (d'après étude Marsch). Selon une étude conjointe d'IFOP et PwC datant de Septembre 2015, moins de 5 % des entreprises françaises ont déjà souscrit à une cyber-assurance.

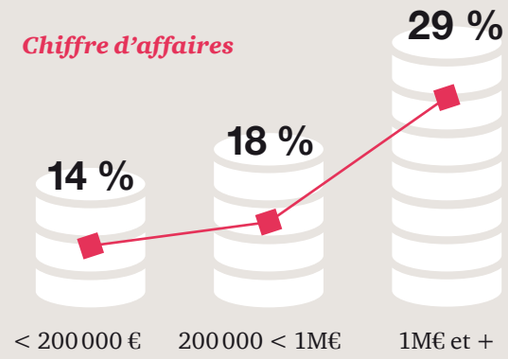
Vous sentez-vous exposé dans votre entreprise au risque de cyber-criminalité (perte de données, usurpation d'identité, manipulation des données confidentielles, ...) ?

Ce taux de souscription, très bas, est principalement dû à la sous-évaluation par les entreprises françaises de leur exposition aux cyber-risques : une majorité (60 %) de dirigeants déclare n'avoir aucune crainte vis-à-vis de la cyber-criminalité. Au total, ce sont 83 % qui se sentent peu ou pas du tout exposés.



Risque d'exposition





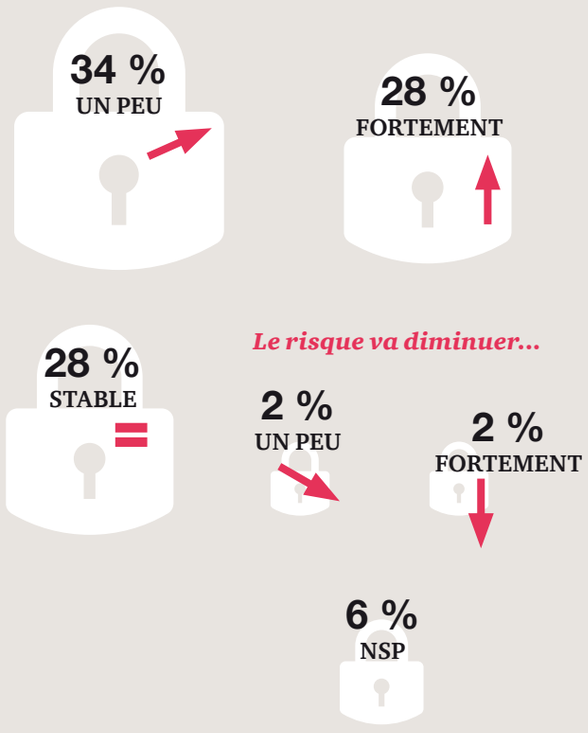
Le risque de cyber-criminalité est aujourd'hui encore peu appréhendé par les entreprises françaises toutes tailles confondues (sachant que le tissu d'entreprises françaises est principalement constitué de TPE/PME) : seules 17 % s'y sentent exposées, principalement au sein des entreprises du secteur industriel. Ce secteur, aux entreprises de taille plus importante et traditionnellement sensibilisées au risque d'intrusions et d'espionnage industriel, se montre plus sensible à cette question : un tiers (32 %) des dirigeants du secteur industriel ressent une vulnérabilité de leur entreprise face à ce risque. De manière plus générale, les entreprises les plus importantes partagent plus largement cette préoccupation : dès le seuil de 1 Million d'euro de chiffre d'affaires, on constate que le pourcentage de dirigeants d'entreprises qui se sentent directement exposés à la cyber-criminalité passe à 29 %.

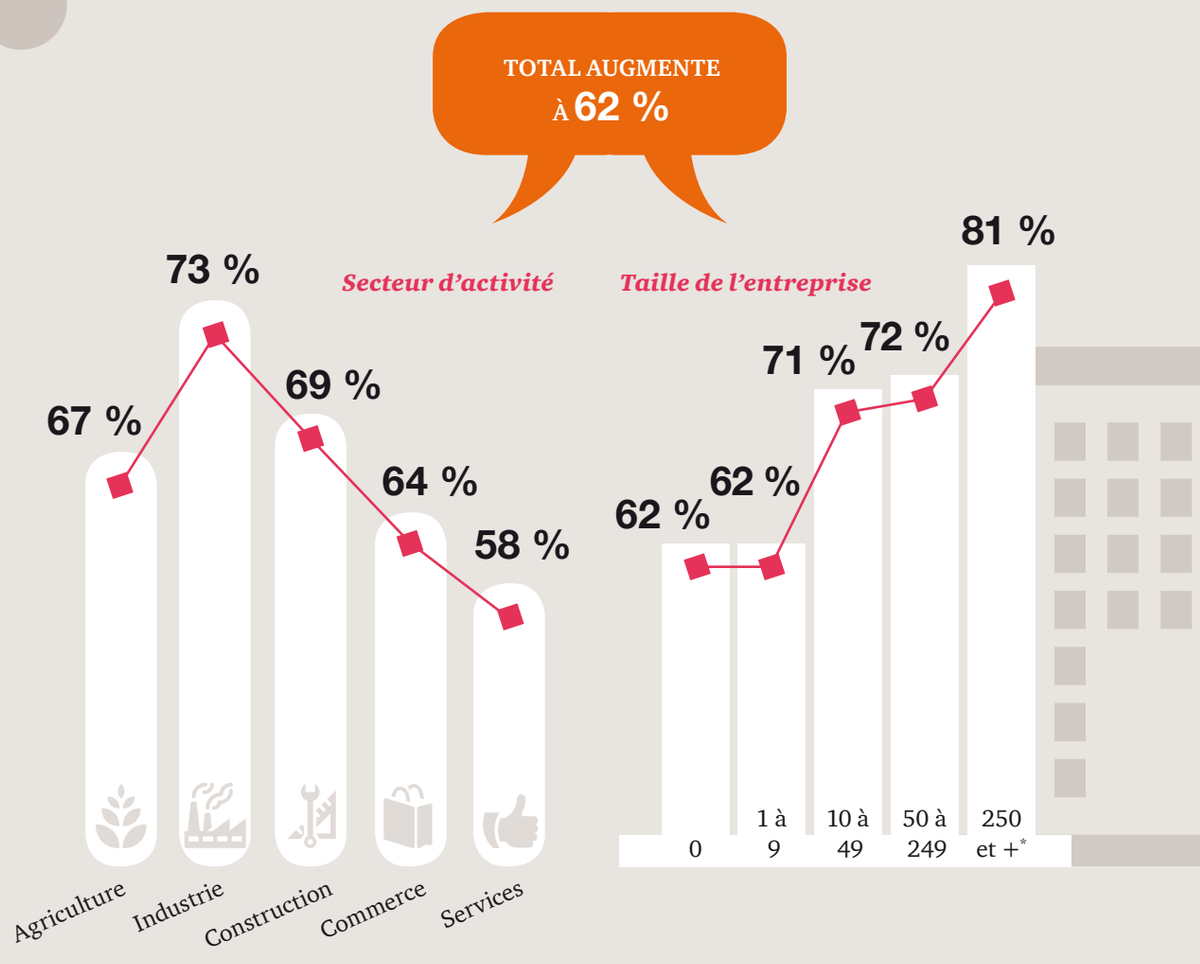
D'après l'idée que vous vous en faites, diriez-vous que le risque pour votre entreprise d'être exposée à de la cyber-criminalité au cours des deux prochaines années va plutôt augmenter ou diminuer ?

Bien que le sentiment d'exposition de son entreprise au risque de cyber-criminalité est encore minoritaire parmi les dirigeants d'entreprise français, une large majorité d'entre eux (62 %) reconnaît que celui-ci va aller en augmentant au cours des prochaines années et ceci de manière importante aux yeux 28 % des dirigeants.

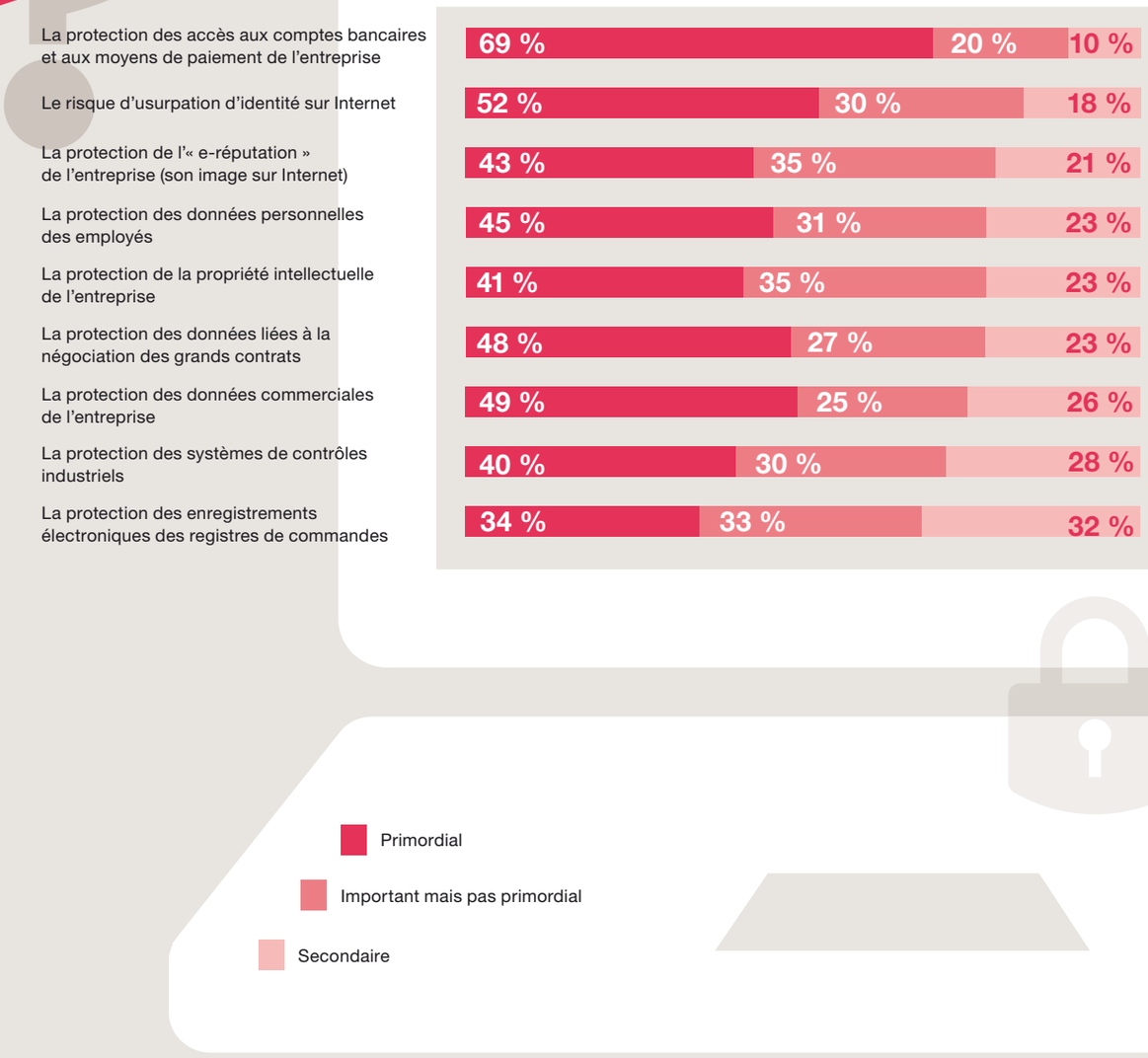
Si ce type de craintes est aujourd'hui plus prégnant parmi les grandes entreprises, ce sont les dirigeants d'entreprises de taille moyenne qui anticipent le plus largement un accroissement de l'exposition aux attaques numériques : un tiers des entreprises comptant de 10 à 49 salariés estime que le risque va fortement augmenter, à l'instar de 42 % des dirigeants de structures employant entre 50 et 249 salariés.

C'est par ailleurs le secteur industriel, d'ores et déjà plus sensibilisé à ce type de risque, qui anticipe le plus largement un accroissement fort de celui-ci : 41 % des dirigeants de ce secteur se prononcent en ce sens.





Pour chacun des risques suivants, veuillez indiquer s'il vous paraît primordial, important mais pas primordial ou secondaire pour une entreprise d'être couverte par une assurance ?



Néanmoins, quel que soit le niveau de risque ressenti, les dirigeants d'entreprise s'accordent largement sur l'importance que revêt la couverture par une assurance des risques associés aux données confidentielles et stratégiques de leur structure.

Deux aspects apparaissent particulièrement sensibles et nécessitent une garantie particulière aux yeux de la quasi-totalité des dirigeants : les comptes et moyens bancaires de l'entreprise (89 % estiment qu'il est important d'être couverts pour le risque d'utilisation frauduleuse de ceux-ci, dont une large majorité – 69 % – qui jugent même cela primordial) et le risque d'usurpation d'identité sur Internet (82 % jugent la couverture de ce risque importante, dont 52 % l'estiment primordiale).

L'ensemble des autres risques présentés (l'e-réputation de la structure, les données personnelles des employés, la propriété intellectuelle de l'entreprise, les données liées à la négociation des grands contrats, au développement commercial de l'entreprise ou au fonctionnement de ses systèmes de contrôle industriels) a également pour les dirigeants d'entreprise une importance stratégique qu'il faut garantir. Les éventuels dommages liés au vol ou à la manipulation frauduleuse de ces données confidentielles constitutives de la vie de l'entreprise sont importants à couvrir pour une très large majorité de chefs d'entreprise : entre 70 % et 78 % d'entre eux s'accordent sur ce point, 4 à 5 dirigeants sur 10 estimant même que cette couverture est primordiale pour chacun de ces risques.

Seule l'importance de protéger les enregistrements électroniques des bons de commande par une garantie d'assurance divise légèrement plus les chefs d'entreprise, qui sont près d'un tiers (32 %) à juger cela secondaire. Une majorité (67 %) estime tout de même qu'il est important de couvrir ce risque.

Les directeurs informatique, sécurité ou achats se montrent légèrement plus préoccupés que leurs directeurs généraux ou PDG vis-à-vis de cette question, et tendent, pour chacun des risques présentés, à accorder une importance plus grande à la couverture de ceux-ci par une assurance.

La couverture des autres risques semble plutôt optionnelle à la majorité des dirigeants : ils sont entre 42 % et 52 % à estimer que chacun d'entre eux peut être couvert, mais à condition d'être inclus dans certaines offres spécifiques. Il est toutefois à noter qu'une proportion non négligeable de dirigeants est convaincue de l'inclusion de ces différents risques dans toutes les polices d'assurance, quelle que soit l'offre choisie. Ainsi les risques liés à l'usurpation d'identité apparaissent-ils couverts par tout type d'offre pour 32 % des responsables interrogés ; il en est de même vis-à-vis de la protection des données commerciales ou liées à la négociation de grands contrats (30 % et 31 % respectivement), ou la protection de la propriété intellectuelle de l'entreprise (28 %).

Pour quelle(s) raison(s) n'avez-vous pas souscrit d'offre de cyber-assurance ?
Base : question posée uniquement aux dirigeants connaissant l'existence des offres de cyber-assurance mais dont l'entreprise n'a pas souscrit une telle offre, soit 33 % de l'échantillon.

51 %

Les risques liés à mes usages d'Internet sont faibles et ne nécessitent pas d'être assurés

39 %

Il ne vous est pas venu à l'esprit de souscrire une offre de cyber-assurance (modalité exclusive)

11 %

Les offres de cyber-assurance ne sont pas suffisamment claires et compréhensibles

6 %

La cyber assurance n'est pas une protection efficace contre la cyber-criminalité

Le potentiel de développement du marché est très élevé au sein des entreprises françaises : 52 % des entreprises interrogées se disent prêtes à souscrire à une police de cyber-assurance alors que seules 5 % en possèdent déjà une.

C'est en premier lieu dans les plus grandes entreprises que les achats de solutions de cyber-assurance sont les plus courants : près d'un tiers des PME comptant entre 50 et 249 salariés a déjà souscrit à une offre spécifique d'assurance. Cette proportion avoisine les 50 % dans les très grandes entreprises : 10 entreprises du CAC 40 sont équipées d'un contrat de cyber-assurance et 9 d'entre elles sont en voie de l'être.

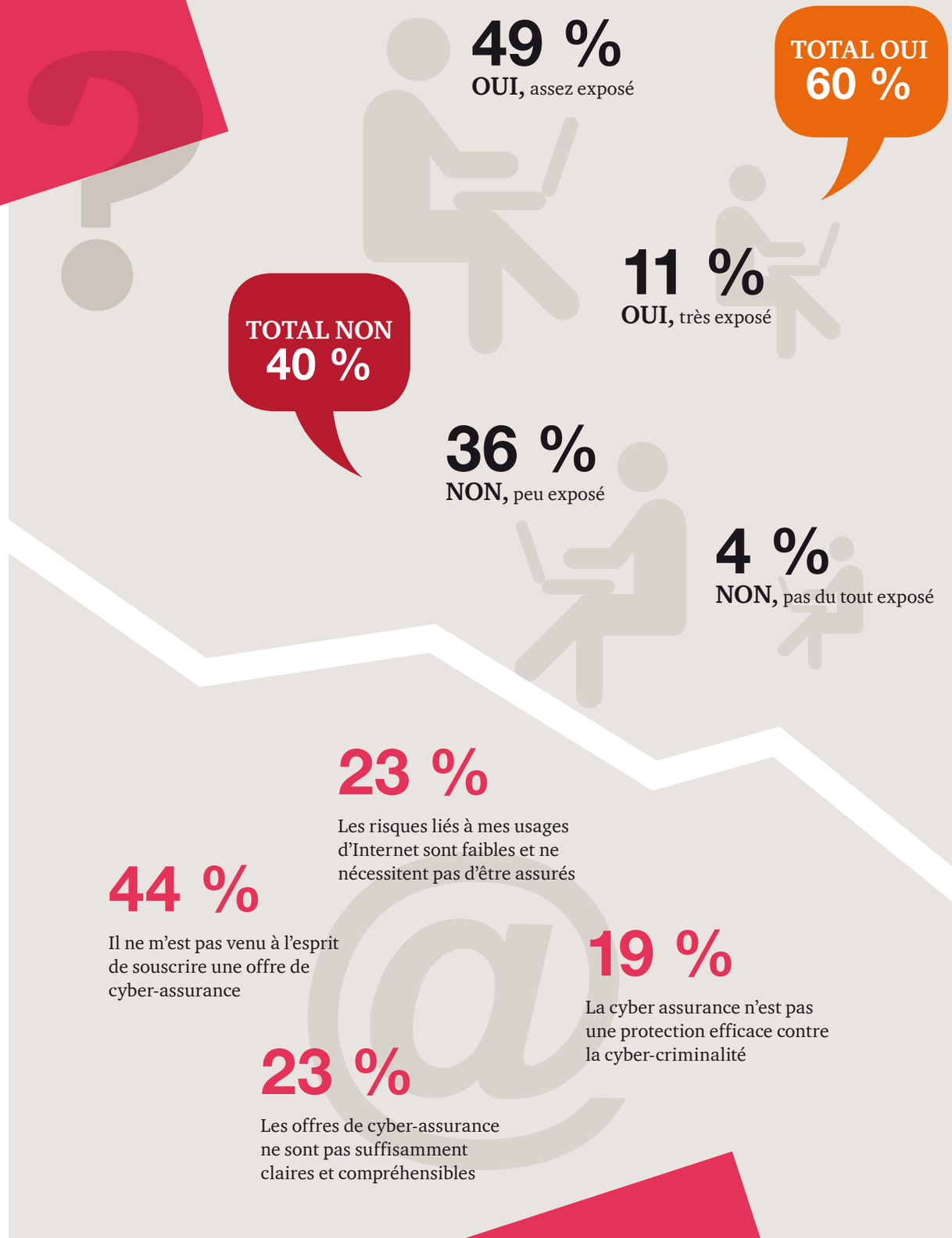
La plupart des dirigeants interrogés n'ayant pas souscrit d'offre de cyber-assurance pour leur entreprise déclarent ne pas en ressentir le besoin (51 %), et estiment le risque trop faible pour engager une dépense de ce type. Une des raisons de cette prise de conscience déficiente tient dans la relégation des responsabilités « cyber » aux seules équipes techniques. Si leur rôle est fondamental, celui des équipes audit-risque et des directions financières l'est tout autant. À la faible conscience de l'exposition de son entreprise aux attaques et fraudes numériques s'ajoute une notoriété réduite de ces offres spécifiques : 39 % des dirigeants n'ont pas souscrit ce type d'offre, non pas parce qu'ils ont le sentiment d'être prémunis contre ces risques, mais parce que cela ne leur est pas venu à l'esprit.

Face au renforcement anticipé du risque de fraudes et d'intrusions Internet, 52 % des dirigeants d'entreprise se déclarent prêts à investir dans une solution de cyber-assurance garantissant leur entreprise, ce qui marque un véritable potentiel de croissance du marché de la cyber-assurance dans les années à venir.

C'est sans surprise au sein des plus grosses structures que le potentiel de développement des offres de cyber-assurance est le plus élevé : 69 % des dirigeants d'entreprise réalisant un chiffre d'affaires d'un million d'euros minimum seraient prêts à consacrer une part de leur budget à cette fin.

Un travail d'évangélisation demeure néanmoins nécessaire auprès de 48 % des dirigeants qui ne voient pas l'intérêt, pour leur structure, d'une telle offre et ne seraient pas prêts à y consacrer une ligne budgétaire, cette proportion s'élevant à plus de la moitié des dirigeants au sein des entreprises individuelles (55 %), ainsi que dans les secteurs du commerce et de la construction, où les micro-entreprises sont nombreuses (respectivement 58 % et 60 %).

Vous sentez-vous personnellement exposé au risque de cyber-criminalité (perte de données, usurpation d'identité, manipulation de vos données personnelles, …) ?



Le potentiel de développement du marché est très élevé au sein des particuliers : 64 % des Français interrogés se disent prêts à souscrire à une police de cyber-assurance alors que seuls 6 % en possèdent déjà une.

Pour se protéger contre les cyber-risques, 24 % des Français seraient prêts à consacrer entre 20 euros et 50 euros par an à une cyber-assurance. Il est intéressant de noter que les particuliers sont plus sensibles aux cyber-risques que les entreprises, puisque 60 % des Français affirment y être exposés (contre 17 % des entreprises, sachant qu'on descend à 14 % pour les entreprises de moins de 200 000 euros de CA, et qu'on atteint en revanche 29 % dès le seuil de 1 million d'euro). Le sentiment d'exposition au risque est nécessairement corrélé, pour partie, au fait d'avoir déjà eu à subir un acte de cyber criminalité : 80 % des particuliers déclarant qu'ils sont exposés à ce risque en ont été victimes dans l'année écoulée.

Si 40 % des Français ne se sentent pas exposés aux cyber-risques, une large majorité (88 %) reconnaît que le risque d'exposition au cours des deux prochaines années va augmenter et ce de manière importante pour 43 % d'entre eux. C'est en région parisienne et chez les moins de 35 ans que le sentiment est le plus partagé. Sans aucun doute, les récents déboires ultra médiatisés de stars ayant subi des violations de vie privée, les interpellent. Il semblerait que lorsque la donnée concerne sa propre personne ou sa famille plutôt que l'entreprise dans laquelle on travaille, le risque qu'elle soit accessible sans son consentement paraît plus élevé.

À l'inverse des entreprises, une minorité des Français (23 %) estime le risque d'exposition trop faible pour engager une dépense de cyber-assurance. Cependant, ces offres spécifiques souffrent d'un manque de notoriété plus grand chez les particuliers que chez les entreprises : 44 % des Français (contre 39 % des entreprises) n'ont pas souscrit à ce type d'offre, non pas parce qu'ils ont le sentiment d'être prémunis contre ces risques, mais parce que cela ne leur est pas venu à l'esprit.

Pour quelle(s) raison(s) n'avez-vous pas souscrit d'offre de cyber-assurance ?
Base : question posée aux personnes connaissant les offres de cyber-assurance et n'en ayant jamais acheté, soit 35 % de l'échantillon.

Une offre non encore mature

Les offres de cyber assurances sont globalement bien perçues mais elles souffrent encore d'un trop grand manque de notoriété

Un effort de commercialisation est à fournir de la part des assureurs pour faire évoluer le marché de la cyber-assurance. 61 % des dirigeants ne connaissent pas l'existence de la cyber-assurance. À ce jour, une minorité d'entreprises se sont déjà vues proposer une telle offre par leur assureur : seulement 33 % des dirigeants disent avoir été contactés au sujet d'une solution de cyber-assurance, dont 17 % à plusieurs reprises. Même son de cloche du côté des particuliers où 41 % des personnes seulement connaissent l'existence de ce type d'offre. Parmi ces derniers, 84 % n'ont jamais été contactés par leur assureur pour se voir proposer des produits de cyber-assurance.

32 %*

Oui, mais je ne connais pas très bien le détail de ce type d'offre

TOTAL OUI 41 %*

9 %*

Oui, et je connais bien le détail de ce type d'offre

*réponses des particuliers

59 %*

Non, je ne connaissais pas l'existence de ce type d'offre

Certaines sociétés ont développé des solutions de cyber-assurance protégeant les assurés contre les risques spécifiques aux usages Internet. Étiez-vous au courant de l'existence de ce type d'offres d'assurance ?

Certaines sociétés ont développé des solutions de cyber-assurance protégeant les assurés contre les risques spécifiques aux usages Internet. Étiez-vous au courant de l'existence de ce type d'offres d'assurance ?

27 %*

Oui, mais je ne connais pas très bien le détail de ce type d'offre

TOTAL OUI 39 %*

12 %*

Oui, et je connais bien le détail de ce type d'offre

*réponses des dirigeants d'entreprise

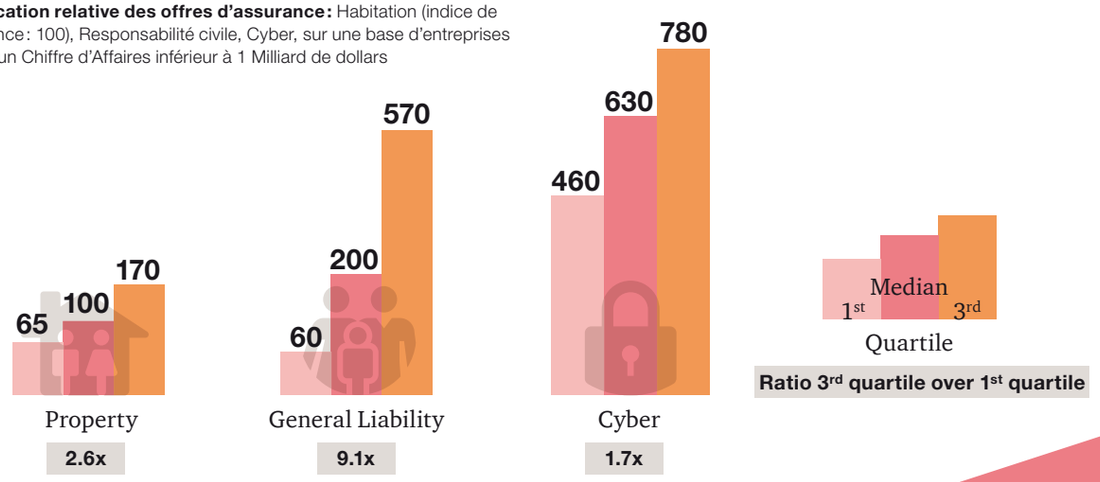
61 %*

Non, je ne connaissais pas l'existence de ce type d'offre

La tarification des offres : Un indice important sur leur manque de maturité

Un signe important du manque de maturité de l'offre, c'est la faible sensibilité des primes d'assurance. Alors que pour les assurances sur la responsabilité civile l'écart de prix peut être d'un rapport de x9.1 entre les polices les 25 % les moins chères, et les 75 % les plus chères, cet écart n'est que de x1,7 sur les polices « cyber risque ». En même temps, le prix absolu des polices semble bien plus élevé sur le risque cyber.

Tarification relative des offres d'assurance : Habitation (indice de référence : 100), Responsabilité civile, Cyber, sur une base d'entreprises ayant un Chiffre d'Affaires inférieur à 1 Milliard de dollars



Les raisons techniques du manque de maturité des offres

Cette difficulté de tarification des offres est due à une conjonction de facteurs : manque de données historiques sur les sinistres et les incidents, réticence des entreprises à partager l'information sur l'impact des cyber-attaques subies, évolution rapide et continue des nouvelles technologies rendant imprévisible le risque encouru. De plus, les cybers attaques n'ont pas toutes les mêmes conséquences sur les systèmes qu'elles affectent. Ces conséquences varient en fonction de la façon dont les entreprises et les particuliers utilisent leurs systèmes d'information. Au final, il n'existe pas de « modèle universel » de modélisation des risques qui s'adapterait à tous les contextes, ce qui en fait une des principales difficultés pour l'assureur à tarifer ces risques.

Cette difficulté à modéliser un risque systémique qui se propage de secteurs en secteurs est bien illustrée par une étude publiée par le Lloyds.

Dans cette étude projective, une cyber attaque sur le réseau électrique nord-américain cause une coupure de courant pour 15 états américains, et plonge dans le noir jusqu'à 93 millions de personnes pendant plusieurs semaines. Les pertes sont évaluées entre 243 millions de dollars et mille milliards de dollars soit plus de 5 % du PNB américain. Le coût est significatif car, en plus de ces conséquences directes, s'ajoutent des conséquences indirectes telles qu'une baisse à moyen et long termes des revenus des compagnies d'électricité sous-traitantes ou des fournisseurs d'électricité provoquant une perturbation de la chaîne d'approvisionnement d'électricité. Les assureurs devront proposer des offres qui tiennent compte du fait que ces conséquences ne seront jamais figées. Les menaces sont très évolutives : des vulnérabilités apparaîtront chaque jour et permettent des nouveaux scénarios d'attaques plus sophistiqués.

À ces difficultés de modélisation s'ajoute le fait que la majorité des incidents ne sont pas liés à la technologie mais à des défaillances humaines organisationnelles. Ces défaillances sont des causes immatérielles qu'il est difficile de prévoir et de quantifier.

Enfin, tant qu'il n'y aura pas de produits de réassurance matures, le marché de la cyber-assurance ne pourra pas se développer à grande échelle.

Une étude publiée par le Lloyds, datant de juillet 2015, « The insurance implications of a cyber attack on the US power grid ».

03

Les leviers du marché

Malgré ces obstacles, le marché connaît une très forte croissance. Le marché a crû au niveau mondial de 85 % entre 2013 et 2014. Il pourrait poursuivre sur une base de 30 %-40 % de croissance par an pour atteindre 10 milliards de dollars en 2020. Llyods évoque même à moyen terme un chiffre de 85 milliards de dollars. La prépondérance technique du risque « Cyber » décrit plus haut constitue en tant que tel le principal facteur de développement.

Une prise de conscience des dommages causés

Deux décisions de justice rendues à l'été 2015 aux États-Unis devraient accélérer la prise de conscience des dommages causés par les cyber-crimes. Dans l'univers de l'entreprise, ces décisions vont accélérer la participation de la direction juridique à la gestion du risque cyber, au côté de la direction informatique et de la direction générale. En juillet, la Cour d'Appel des États-Unis a reconnu la responsabilité civile du distributeur Neiman Marcus dans la fuite de données qui a touché 350 000 clients – dont plus de 9 000 comptes ont par la suite fait l'objet de fraudes. C'est la première fois qu'une Cour d'Appel aux États-Unis reconnaît les dommages subis par les consommateurs sur leurs comptes de cartes crédits à la suite d'une fuite de données. En août, suite au procès intenté par la Federal Trade Commission contre l'opérateur hôtelier Wyndham Worldwide Corp, la troisième cour d'appel de la juridiction de Philadelphie a décidé que la FTC aurait toute latitude pour réguler les compagnies privées qui mettraient en danger les données de ses clients et utilisateurs. Ces décisions vont mettre au centre des analyses d'écarts les standards de cyber-sécurité publiés par la NIST en 2014 (« NIST Cyber Security Framework »). Ils constitueront aussi des adjuvants importants au développement du marché de la cyber-assurance aux États-Unis.

Mais pas seulement pour les États-Unis : n'importe quel fournisseur ou prestataire de service d'une société américaine, et donc potentiellement vecteur d'un risque cyber pour cette société, pourrait avoir rapidement à faire la démonstration qu'elle suit les meilleures pratiques de son client – c'est-à-dire, entre autre, suit à minima le NIST Cyber Security Framework et a souscrit à une police de cyber-assurance. Ce dernier point limiterait les risques encourus par chaque partie. En particulier, il pourrait rassurer un client américain sur le choix d'un fournisseur étranger qui de facto répond aux standards US et qui a garanti sa pérennité.

En Europe, la Commission a adopté en 2013 une directive proposant d'améliorer le niveau de cyber-sécurité. La proposition est pour le moment en cours d'examen devant le Conseil. Dans sa version actuelle, la directive ne concernerait que les opérateurs d'infrastructure essentielle dans de multiples secteurs (services financiers, santé, transports, énergie), les sociétés de services informatiques, les administrations publiques, et exclurait les micro-entreprises. La directive propose trois mesures qui pourraient catalyser le marché de la cyber-assurance :

- elle dispose que les entreprises concernées doivent s'organiser et se protéger contre les risques menaçant la sécurité des réseaux et de l'information (SRI) ;
- si le système d'information a subi des dommages qui pourraient mettre en danger la sécurité d'un réseau et la continuité d'opérations essentielles, les organismes se verraient dans l'obligation de notifier l'incident aux autorités compétentes qui, à leur tour, auront la possibilité de prévenir le public ;
- les autorités compétentes pourraient exiger de la part des entreprises qu'elles fournissent des preuves de la mise en œuvre de politiques de sécurité et qu'elles se soumettent à un audit.

Or, à date d'aujourd'hui, une minorité d'entreprises françaises a mis en place des mesures et outils spécifiques pour se protéger d'intrusions et attaques numériques auxquelles elles ne se sentent, pour la plupart d'entre elles, pas exposées. Si le fait de disposer d'un logiciel anti-virus standard est courant (71 % des entreprises en sont dotées), plus rares sont les structures qui ont mis en place des outils de sécurité renforcée spécifiques. Seul un tiers des entreprises a opté pour des solutions renforçant la sécurité des identifiants sur Internet. Les outils plus « pointus », comme les audits techniques ou comportementaux réguliers, les solutions de type « fireye », les « red team » sont également peu répandus encore au sein des entreprises françaises : ces solutions ont été mises en place dans moins d'un quart des entreprises (au sein respectivement de 23 %, 22 % et 18 % des structures). Les entreprises les plus importantes (disposant d'un chiffre d'affaires supérieur à 1 million d'euros), plus sensibilisées aux risques, sont également celles qui ont plus largement mis en place certains de ces outils spécifiques : 42 % procèdent à des audits réguliers de leurs outils techniques, procédures et comportements et 37 % ont mis en place des solutions de type « fireye ».

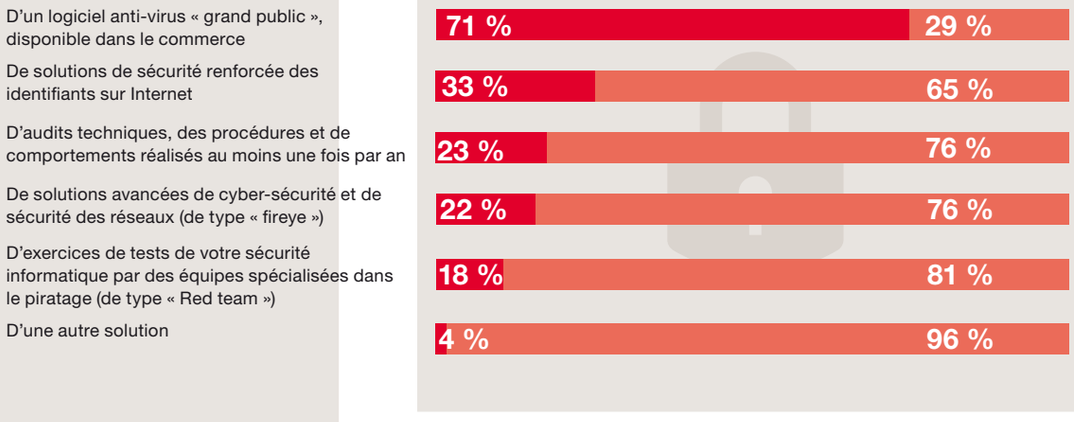
Des rapprochements entre assureurs et acteurs de la cyber-sécurité

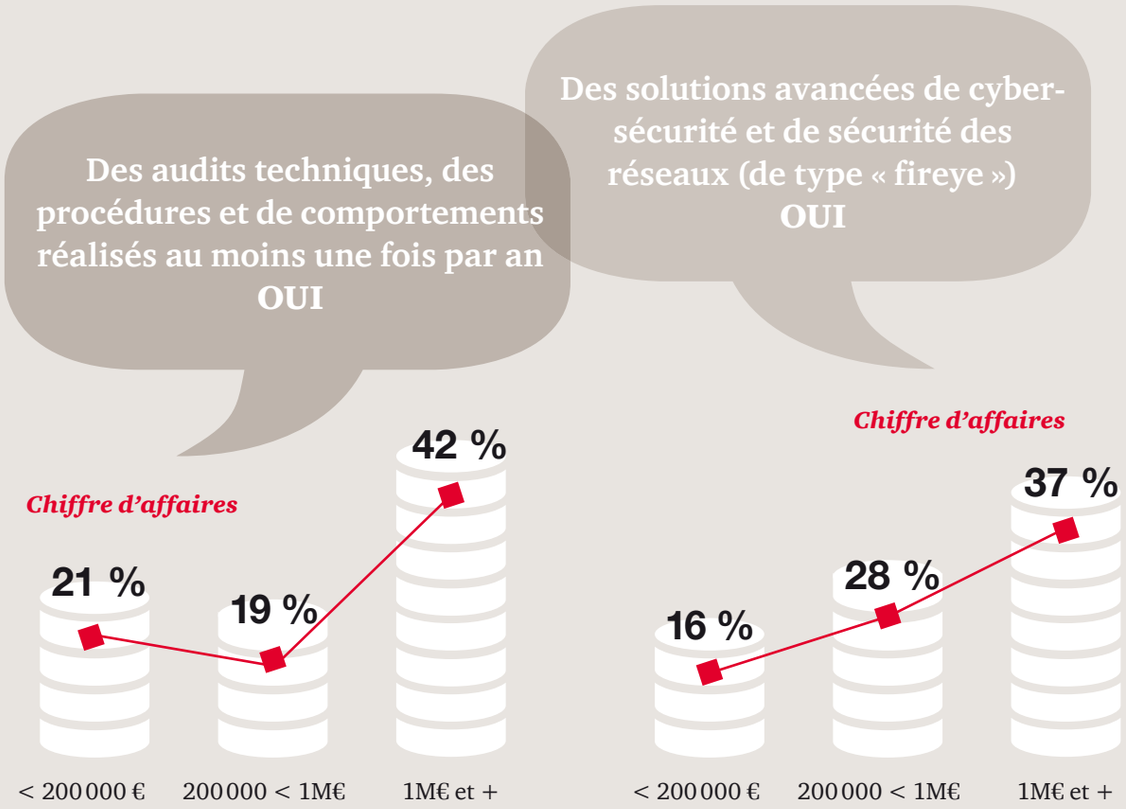
Dans ce contexte, les solutions d'assurance issues d'un partenariat entre un assureur et un spécialiste de la cyber-sécurité, tel Axa et Airbus ou Allianz et Thalès, s'avèrent particulièrement attractives. En effet, elles proposent deux volets : un contrat d'assurance qui couvre les dommages subis suite à une cyber-attaque et un accompagnement en ingénierie sur mesure pour aider les entreprises à se protéger contre les cyber-risques. Des solutions complètes qui pourraient permettre de répondre aux exigences de la directive et à son objectif : renforcer la cyber-sécurité en Europe.

Ce rapprochement entre assureurs et acteurs de la cyber-sécurité est d'autant plus souhaitable que dans les faits, assurer les risques cyber génère des comportements vertueux vis-à-vis de la bonne « cyber-hygiène » de l'entreprise. La mise en place de polices de cyber-assurance impose naturellement avec plus de rigueur des dispositifs de contrôle et facilite les investissements en matière de surveillance des systèmes. De manière générale, les entreprises assurées connaissent un nombre significativement plus réduit d'incidents de cyber-sécurité.

C'est donc une nécessité vitale pour tout cadre dirigeant de l'industrie de l'assurance d'avoir une vision de plus en plus large des partenaires éventuels dans le développement des offres de cyber-assurance - En particulier, les possibilités de s'allier dans la création d'offres nouvelles, mais aussi dans leur distribution, avec les fournisseurs de solutions de cyber-sécurité. Évidemment, si le point de distribution devient un élément de différenciation, et si le risque cyber devient effectivement central à l'analyse générale du risque, alors il ne serait pas étonnant à terme de voir des rapprochements de nature capitalistiques entre grandes compagnies d'assurance et géants de la cyber-sécurité. Ces rapprochements pourraient aussi s'opérer à un coût moindre et de manière plus graduelle en co-développant des solutions ou des standards avec des start-ups ou de jeunes entreprises de la cyber-sécurité en forte croissance.

De quelle manière protégez-vous votre entreprise aujourd'hui contre le risque de cyber-criminalité ? Disposez-vous… ?





04

La cyber-assurance : un marché « stratégique » pour les assureurs

Cyber-assurance et digital : des similitudes sur l'évolution des marchés

L'état actuel du marché – niveau confidentiel, offre encore immature, croissance explosive, compréhension générale d'un potentiel très important – fait écho à l'histoire de nombreux autres marchés digitaux. Le marché du « paid search », initié par Google AdWords, ne dépassait pas les 100 millions de dollars en 2001. En 2014, il pèse autour de 55 milliards de dollars. Il s'agit là d'une évolution désormais « classique », même si tous les marchés en ligne ne décollent pas au même instant. Si la publicité et la réservation en ligne sont des marchés précurseurs avec au moins 10-15 ans d'historique, la disruption digitale de location entre particuliers ou du pooling d'actifs financiers est beaucoup plus récente. Ainsi, le marché de la « Fintech » ne décolle réellement qu'en 2014 avec un brusque triplement des investissements. Ces récentes évolutions contribuent au développement d'un écosystème favorable au décollage des investissements dans la cyber-assurance. Ils constituent aussi de nouveaux risques stratégiques pour les acteurs existants.

L'histoire récente des secteurs précurseurs montre avec quelle vitesse et intensité la valeur dans une filière peut migrer au profit des nouveaux intervenants digitaux. La domination du paid search par une seule société, Google, dont elle tire l'essentiel de ses revenus, constitue l'une des raisons expliquant la tentative de fusion entre Publicis et Omnicom. Sur la base de cette domination sur une seule verticale du marché plus large de la publicité, Google obtient aujourd'hui une valorisation totale dix fois supérieure à celle de Publicis et Omnicom réunis. Le même phénomène peut être vu dans la réservation en ligne pour l'hôtellerie : Priceline, qui ne possède en propre aucun actif et qui est agnostique en terme de réseau, commande aujourd'hui une valorisation boursière presque sept fois plus importante que la chaîne hôtelière Accor, malgré l'accès exclusif de cette dernière à plus de 500 000 chambres – sur la base d'une marge opérationnelle avant amortissement trois fois plus élevée chez Priceline par rapport à Accor.

Marc Andresseen, le fondateur de Netscape, avait écrit en 2011, que « Software is eating the world » - le logiciel engloutit tout. Dans les faits, les nouvelles activités digitales font rarement disparaître les acteurs industriels précédents qui ont développé de fortes relations clients, en particulier lorsqu'elles sont B2B. Publicis, Omnicom, Accor (pour lequel la clientèle d'affaires est critique) sont toujours là. En revanche, la couche de données et de logiciels qu'ils maîtrisent finit par capter l'essentiel de la valeur, dans des rapports qui peuvent aller de 1 à 10.

Le cyber risque : future pierre angulaire de l'ensemble des offres d'assurance

Ces effets de migration risquent d'être encore plus accentués dans l'assurance avec l'irruption de la cyber-assurance. Son importance sera d'autant plus forte qu'elle reflétera la migration de valeur par le digital sur l'ensemble de l'économie illustrée plus haut. Assurer les opérations digitales d'un Priceline ou d'un Google, aux valorisations très significatives, sera plus critique que celles de leurs concurrents plus anciens, moins digitalisées et aux valorisations beaucoup plus faibles. En outre, les effets de la numérisation et de l'automatisation eux-mêmes vont considérablement réduire l'exposition aux risques plus traditionnels, non-cyber. De nombreux responsables dans le secteur de l'assurance auto ont déjà identifié que le développement des voitures sans pilote et la réduction du risque d'accident d'origine humaine – responsable de 90 % des accidents – finirait par provoquer une contraction du chiffre d'affaires liées aux polices d'assurance peut-être jusqu'à 50 % en 2025, et jusqu'à 80 % quinze ans plus tard. Mais ce raisonnement pourra s'appliquer également à la domotique ou encore à l'ensemble des applications de villes intelligentes – de la détection d'incendie ou de ruptures de canalisations aux phénomènes de criminalité. De manière générale, tout comme dans l'automobile, le risque venant de l'erreur humaine va considérablement se réduire (sans pour autant disparaître) au fur et à mesure du développement de systèmes d'alertes avancées, de systèmes prédictifs et du remplacement des gestes humains par des systèmes autonomes. La part des risques « traditionnels », couverts habituellement par les assurances, va s'en retrouver considérablement amoindrie en termes de valeur.

En parallèle, l'exposition au risque lié à la sécurité et la fiabilité de ces systèmes gérés depuis le « cyber » va être relativement plus importante. En conséquence, dans un univers où le risque humain deviendra marginal, la vente de garanties d'assurance couvrant explicitement le risque cyber deviendra nécessaire à la vente de la police : sans elle, la couverture par l'assurance sera médiocre, voir inutile. La couverture du risque cyber va devenir l'un des piliers fondamentaux de la plupart des polices – et peut-être, à terme, le plus important des piliers.

Dans les faits, les années 2013-2015 marquent le début d'une compétition dans le domaine de la cyber-assurance. L'objectif à terme de cette compétition sera de prendre le contrôle de la couche de données et de logiciels qui générera la plus grande croissance de valeur. Cette compétition est trop récente pour avoir un ou plusieurs champions. Il n'existe pas d'équivalent dans la cyber-assurance d'un Google, Apple, Amazon, AirBnB, Netflix, Priceline, Uber, LendingClub… c'est-à-dire un leader qui aura su identifier sur un espace émergent à très fort potentiel le mix produit/service le plus innovant, et bâtir un nouveau marché adjacent, captant l'essentiel de la valeur de toute la filière. Mais l'histoire des transformations digitales, ainsi que les évolutions du domaine de l'assurance, peut permettre d'identifier certaines caractéristiques des futurs leaders de la cyber-assurance.

Marc Andresseen, le fondateur de Netscape, avait écrit en 2011, que « Software is eating the world » - le logiciel engloutit tout.

05

Les caractéristiques des futurs leaders de la cyber-assurance

Devenir expert dans la collecte et l'analyse de la donnée

Les principaux leaders digitaux dans leurs verticales ont compris l'importance de la collecte de donnée comme un des points clés de différenciation. Dès ses débuts, Amazon a su bâtir pour chaque utilisateur un environnement riche d'information. Netflix a fait de même – ainsi que des sociétés comme Google ou Apple qui ont fait des identifiants d'inscription Google-Mail/ Google+ ou iTunes des instruments de collecte systématique de l'information utilisateur. Or, curieusement, la collecte de données est l'une des pierres d'achoppement de la cyber-assurance, un point souligné par de nombreuses études et illustré dans les faits par la faible variabilité du tarification des polices. Au-delà de certaines difficultés techniques liées à des caractéristiques souvent différentes, dans le cadre d'environnement logiciel et hardware toujours en évolution permanente, il y a surtout le refus de nombreuses entreprises d'admettre qu'elles ont été victimes d'attaque, un point mis en avant, entre autre, par Suzanne Spaulding du Department of Homeland Security. Les futurs leaders de la cyber-assurance seront capables de collecter toutes les données sur les anomalies techniques, erreurs de comportements, absences de procédures… commises par les employés d'entreprises cibles tout en préservant la confidentialité de ces informations pour le compte des entreprises clientes, dans le cadre des responsabilités et devoirs de chaque acteur vis-à-vis des autorités nationales de régulation. Il y aura là deux capacités importantes : en amont, celle de cartographier les systèmes informatiques, mais aussi les protocoles en place et les comportements des utilisateurs humains ; en aval, la capacité d'échanger avec des réseaux d'information et d'alertes dédiées à la cyber-sécurité – l'ensemble préservant la confidentialité de chaque agent. Une première ébauche de ce type de capacité a été décrite dans un rapport récent du Department of Homeland Security, sous le concept de « Cyber Incident Data Repository », qui pourrait être opéré par n'importe quel agent privé.

Ce type de réservoir de données, structurées ou non, devrait également être

alimenté par les informations de renseignement plus ou moins privilégiées obtenues soit par des agences privées – comme par exemple iSight Partners, ou bien les services correspondants, plus ou moins informels, de prestataires tels que par exemple Symantec, Crowdstrike, Intel Security Unit…. – ou bien même via les services de sécurité de l'État. Au final, toutes ces données devront être communiquées via des standards pour l'échange automatisé d'information tels que par exemple TAXII, STIX et CybOX, aujourd'hui promues aux États-Unis par le Department of Homeland Security.

Cependant, collecter la donnée en tant que tel n'apporte pas de valeur. Amazon a investi dans la connaissance client afin de développer ses algorithmes de recommandation et augmenter la satisfaction client, tout en identifiant au mieux la rentabilité de chaque produit. Netflix a créé un prix Netflix entre 2007 et 2009, doté d'un million de dollars, afin que des équipes de recherche puissent améliorer la précision des algorithmes de « collaborative filtering » pour servir les meilleures recommandations à chacun des membres de sa base utilisateur. La capacité de quantifier le risque, qui est au cœur du métier de l'assurance, nécessitera de développer des modélisations toujours plus complexes au fur et à mesure de l'imbrication et de l'importance grandissante prise par les réseaux digitaux. L'étude récente de la LLoyds avec le Cambridge Centre for Risk Studies sur une situation de blackout suite à une attaque sur le réseau de distribution électrique aux États-Unis indique une des directions de ce type de modélisation : des simulations complexes, faisant appel à de multiples sous-scénarios, et qui devront être eux-mêmes réactualisés au fil d'un environnement technologique en constant « upgrade ». Ces vastes analyses capables d'associer une échelle de coûts à un risque, serviront elles-mêmes de « baseline » pour générer une deuxième couche d'information : un scoring des entreprises, des infrastructures, voir des procédures et comportements internes, permettant de synthétiser ces analyses de risques et d'échanger de manière plus simple sur l'évaluation du risque de chaque composant de la chaîne de la valeur. C'est par exemple le type de services aujourd'hui délivré par la société BitSight, capable de donner un scoring sur la qualité d'une entreprise en termes de couverture de son risque cyber. Ce type de scoring est amené à se développer et à se raffiner : on pourra faire un scoring de procédures, de comportements, de choix logiciels et matériels en même temps que l'on pourra obtenir un scoring d'un certain écosystème d'entreprises régionales ou sectorielles – ces scores servant d'input simplifiés aux modèles de risques.

Réinventer la tarification, la distribution et in fine le business model

L'univers cyber va certainement transformer les modalités de tarification, services, distribution et investigation après événement déclencheur des polices de cyber-assurance.

Une prise en compte beaucoup plus précise du facteur temps devra être réalisée. Pour la plupart des particuliers, nombre des outils et actifs utilisés vont être facturés de manière de plus en plus importante en temps d'usage – une transformation profonde permise par le digital, qui autorise la cessation temporaire de droits d'utilisation et qui trouve son expression, aujourd'hui dans l'économie collaborative, demain dans le déploiement de flottes de véhicules sans pilotes, de systèmes autonomes et d'appartements de type « smart home ». Pour le particulier qui ne possède pas l'actif, la couverture à l'exposition du risque d'utilisation prendra sens uniquement lors de la durée d'utilisation. Cette limitation devra être prise en compte dans la tarification de polices d'assurances liées à l'utilisation temporaire de tel ou tel actif. En outre, une modélisation continue des phénomènes cyber dans le cadre d'un environnement en constante évolution pourrait donner lieu à des réévaluations des primes en temps réel sinon pour le particulier, du moins pour les marchés de réassurance.

La tarification elle-même pourrait évoluer en fonction de la mise en place des systèmes informatiques ainsi que des procédures et des comportements appropriés permettant de réduire le risque cyber. Ce type d'approche est déjà testé dans le domaine de l'assurance santé aux États-Unis par des opérateurs tels que l'assureur Cigna, dans le cadre du programme de distribution de bandeaux connectés BodyMedia permettant de mesurer des données de santé, ou plus largement dans le marché de l'automobile avec le pay as/how you drive qui existe de part et d'autre de l'atlantique y compris en France. BP a également déployé un programme de réduction de la police d'assurance pour ses employés en fonction de leur activité physique mesuré avec FitBit. Si une mesure fiable, en temps réel, de l'environnement général de cyber-sécurité peut être obtenue pour une entreprise, alors des programmes de réduction du coût des polices de cyber-assurance pourront être établis au fur et à mesure de la réduction du risque de cyber-sécurité. L'assureur pourrait à l'occasion conseiller ou distribuer les méthodes, procédures, technologies et programmes de transformation comportementale permettant d'atteindre une réduction du risque de cyber-sécurité, sur la lignée des programmes de prévention que développent de plus en plus les assureurs, que ce soit en prévoyance collective, santé ou auto.

Des pratiques à emprunter à l'industrie aéronautique…

L'investigation des causes de l'événement déclencheur pourrait, elle, s'avérer beaucoup plus complexe. Si l'on prend le cas de la voiture sans pilotes comme exemple avancé de la transformation par l'internet des objets et les systèmes autonome, on peut poser l'hypothèse que très peu d'accidents seront dus à une origine strictement humaine (même si les expériences des voitures sans pilotes Google montrent que les voitures où l'être humain peut reprendre rapidement le contrôle peuvent être dangereuses). Si un accident est dû à un « bug » – qui a émergé de manière accidentelle ou bien a été introduit pour raisons malveillantes – l'analyse des responsabilités ressemblera aux investigations dans l'aéronautique après un accident : quel enchaînement d'erreurs informatiques est à l'origine de l'accident ? Les responsabilités pourraient être multiples et diverses. Si l'accident survient à la suite d'un ver informatique diffusé dans le système automobile via le smartphone Android ou IoS de l'utilisateur, infecté par un maliciel d'origine étrangère mais dont l'intention n'était pas le crash de la voiture, qui est responsable ? L'échange d'information rapide sur les investigations de cas similaires constituera un besoin critique afin d'assurer la meilleure qualité d'investigation des accidents avec des coûts maîtrisés.

…ainsi qu'aux champions numériques des effets de réseaux

Cet échange d'information rapide, constituant un avantage concurrentiel, met en valeur la capacité des futurs champions de la cyber-assurance à être des acteurs de réseaux performants. Cela veut dire être capable de développer des standards les plus ouverts possibles mais aussi trouver des formes de partage de la valeur qui puissent intéresser le plus grand nombre possible de participants.

Ce point rend critique la réflexion sur la distribution et le déploiement de tous ces services d'assurance, qui pourraient être différents de ce qui se fait aujourd'hui. Un avantage commercial important pourrait être acquis à l'assureur qui offre une vision synthétique au particulier ou à l'entreprise de son exposition au risque de cyber-sécurité, évoluant en temps réel, et démarrant du diagnostic initial à la mise en place réussie ou non des technologies, procédures et comportements permettant la réduction de ce risque. Le design de cette représentation, son aspect intuitif et immédiatement pertinent, ne sont pas des éléments triviaux, bien au contraire : les réussites de sociétés telles qu'Apple ou Dropbox soulignent l'importance stratégique d'un design de service qui réponde bien aux besoins d'information de l'utilisateur tout en paraissant le plus simple possible.

Une distribution ouverte au plus grand nombre, déployée de la manière la plus rapide et donc la plus simple possible, sera également critique afin de maximiser les effets de réseaux qui constituent les avantages compétitifs les plus critiques des grands leaders du monde digital. Google, Facebook ou, à plus petite échelle dans le B2B, SurveyMonkey ont pu imposer leur standard en s'attaquant non pas à des grands comptes avec des offres ultra-personnalisées et disposant d'un accompagnement humain, mais au contraire en se développant avec des offres « libre services », disponibles pour tout type d'organisation de manière totalement automatisée. Un avantage compétitif sera obtenu pour toute offre autour de la cyber-assurance capable de s'évaluer et de s'acheter en « libre-service » – même s'il ne s'agit pas de la police d'assurance elle-même. À nouveau, cet avantage aura également un effet important dans le métier même de la gestion du risque cyber. En termes d'analyse de la propagation du risque sur un ensemble d'acteurs de toutes tailles mais tous reliés – particuliers, TPE, PME, grands groupes… – les acteurs ayant été capables de se positionner sur ces réseaux seront ceux qui auront la meilleure vision, obtenue le plus rapidement, de la dangerosité et vitesse de propagation de tel ou tel maliciel.

S'ouvrir à de nouvelles opportunités hors des métiers « traditionnels » de l'assurance

On le voit bien dans ce qui précède, la chaîne de valeur de la cyber-assurance va faire émerger sinon de nouveaux métiers, du moins de nouvelles activités : audit ultra rapides des environnements internes ; dashboard synthétique de l'état du risque cyber ; scoring d'entreprises, mais aussi de technologies, de procédures et de comportements humains ; entrepôt de données sur les incidents de cyber-sécurité ; moteurs complexes de simulation et de quantification ; réseaux d'échange d'information sur les incidents de cyber-sécurité ; programmes intégrés de réduction du risque cyber liant l'identification des sources de risques à des efforts sur mesure d'éducation, prise de conscience, changements procéduraux, développement de stratégies de réponse via de nombreux outils dont par exemple les exercices terrain/red-team, mais aussi la mise à disposition de services de gestion déléguée du risque cyber ; marchés en temps réel de réassurance et donc automates de trading d'assurance… Cette liste non exhaustive de futures opérations recèle peut-être des activités critiques à terme dans l'établissement des polices, et donc capable de capter une part significative de la valeur comme cela a été vu dans d'autres industries (par exemple, la réservation en ligne dans l'hôtellerie) ; ou tout simplement identifie de nouvelles activités adjacentes qui se transformeront petit à petit en domaine stratégique de captation de la valeur comme cela s'est vu à nouveau ailleurs (par exemple, le marché du « paid search » dans l'univers publicitaire). Il serait plus qu'hasardeux à date de mettre le doigt sur l'une de ces activités en priorité. Nul doute qu'un gestionnaire de fonds VC, ou un technologue, y verrait là une suite d'évolutions de la valeur qui seront autant de paris dont la réussite dépendra d'un des facteurs les plus critiques pour le succès d'une start-up, comme le soulignait récemment Bill Gross, le patron de l'accélérateur Idealab : le timing.

Les cadres dirigeants en charge du développement de la cyber-assurance découvriront également de nombreux nouveaux business models hors de leurs activités traditionnelles – qui seront autant d'opportunités mais aussi de risques en termes de focus managérial. D'une part, si les fournisseurs de solutions de cyber-sécurité deviennent des partenaires importants, peut-être aussi les données collectées par les cyber-assureurs pourraient-elles donner un avantage à ces mêmes fournisseurs – par exemple dans l'identification des meilleures technologies, procédures et programmes de transformation des comportements humains permettant la réduction du risque de cyber-sécurité, au meilleur coût. On peut ainsi très bien imaginer une inversion du rapport de force, et faire du cyber-assureur l'acteur central de la cyber-sécurité de par sa capacité à terme à chiffrer, conseiller et donc orienter la distribution. Il s'agit l'un d'un embranchement stratégique possible : la cyber-sécurité comme le futur de la cyber-assurance. D'autres sources de création de valeur sont également possibles. La capacité de simuler des risques au niveau d'une entreprise, d'un écosystème industriel ou d'un type d'infrastructure, et d'en voir les effets chiffrés sur d'autres secteurs industriels – voilà qui peut constituer également beaucoup de valeur pour de nombreux acteurs externes, de la banque d'affaires aux instituts de prévisions économiques publics ou privés, voir mêmes aux industries de la défense. Pour un acteur dominant, les champs qui s'ouvriront en terme de création de valeur pourraient être assez larges – ce qui peut représenter d'ailleurs un risque de dilution du focus managérial. C'est l'une des raisons qui explique par exemple la récente réorganisation de Google en « Alphabet ».

Pour l'acteur prêt à prendre un risque, à expérimenter, à coopérer – dans une approche nouvelle de collecte et d'analyse des données ; dans l'exploration de nouveaux business models/ nouvelles formes de tarification ; dans le développement d'offres simples d'apparence et diffusées au plus grand nombre ; dans l'ambition de devenir un véritable acteur de réseau ; et dans la témérité à aller chercher des clients venant de secteurs qui lui étaient encore inconnus – il y a là la promesse de se hisser au plus haut rang du marché de la cyber-assurance, un marché encore très jeune mais aujourd'hui en croissance extrêmement forte.

Sources externes

Pourquoi le risque cyber devient central pour nos économies

- "The Global State of Information Security® Survey 2016 - Turnaround and transformation in cybersecurity", PriceWaterhouseCoopers (2015) – voir : http://www.pwc.fr/the-global-state-of-information-security-survey-2016-turnaround-and-transformation-in-cybersecurity.html ;
- " Software Failures of 2014 : Transportation Edition", Tricentis (2015) ;
- "Net Losses : Estimating the Global Cost of Cybercrime", Intel Security/McAffee/CSIS (2014) ;
- "The decline of the British bank robber", British Bankers' Association (2013) ;
- "Hackers Steal $1 Billion In Biggest Bank Heist In History : Could They Take Down The Whole System Next Time ?", International Business Times (16/02/2015) ;
- "Russia's "Crime-as-a-service" Exposed – Just Look At What You Can Buy", SiliconAngle (5/11/2012) ;
- Estimations marché mondial cybersécurité : Gartner (2015) & Markets & Markets (2015) – voir également "The Global State of Information Security® Survey 2016 - Turnaround and transformation in cybersecurity", PriceWaterhouseCoopers (2015) ;
- " Die Lage der IT-Sicherheit in Deutschland 2014", Bundesamt für Sicherheit in der Informationstechnik (2015) ;
- "New Havex malware variants target industrial control system and SCADA users", PCWorld (24/06/2014) ;
- Analyse évolution zero-days : d'après base de données National Insitute of Standards Technology (voir https ://web.nvd.nist.gov/view/vuln/) ;
- "Boeing 787 software bug can shut down planes' generators IN FLIGHT", TheRegister (1/5/2015) ;
- "After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix", Wired (24/07/2015) ;
- "Government Will Actually Spend $330 Million To Protect Victims Of The Opm Hack", NetxGov (2/09/2015) ;
- "How much do data breaches cost big companies ? Shockingly little", Fortune (27/03/2015) ;
- "À 2015 Survey : Cybersecurity in the boardroom", NYSE Governance Services (2015) ;
- "Cybercrime Will Cost Businesses Over $2 Trillion By 2019", Juniper Research (12/05/2015).

La cyber-assurance : un nouveau marché encore limité à très haut potentiel

- Christian Biener, Martin Eling, Jan Hendrik Wirfs, "Insurability of Cyber risks : an empirical analysis", University of St. Gallen, 2015 ;
- "Why cyber-insurance will be the next big thing", CNBC (1/07/2014) ;
- "Global Insurance Market Opportunities ", Aon Benfield Analytics (2015) ;
- "UK Cyber Security : the role of Insurance in managing and mitigating the risk", Marsh (3/2015) ;
- "The Insurance implications of a cyber attack on the US Power Grid", Lloyds (07/2015).

Les leviers de Marché

- “Here’s why the cyber insurance industry is worth £55.6 billion”, ItProportal (07/02/2015) d’après rapport du Barbican Insurance Group, Llyod’s ;
- “Risks to Drive US$10 Billion Cyber Insurance Market by 2020”, ABI Research (29/07/2015) ;
- “Companies, Seeking Common Ground on Cybersecurity, Turn to Insurers”, Wall Street Journal (13/04/2015) ;
- “Appeals Court Revives Neiman Marcus Data Breach Suit” ,Wall Street Journal (23/07/2015) – voir aussi commentaires à HYPERLINK « https ://www.sans.org/newsletters/newsbites/xvii/57 » \l « 200 » https ://www.sans.org/newsletters/newsbites/xvii/57#200 ;
- “What CIOs Need to Know About the FTC Cybersecurity Ruling”, Wall Street Journal (31/08/2015).

La cyber-assurance : un marché stratégique pour les assureurs

- « Internet Ad Spend To Reach $121B In 2014, 23 % Of $537B Total Ad Spend, Ad Tech Boosts Display”, TechCrunch (7/04/2014) ;
- “The Evolution of Google AdWords – A $38 Billion Advertising Platform”, WordStream (05/06/2012) ;
- “The fintech revolution” ,The Economist (9/05/2015) ;
- “The future of fintech and banking”, Accenture (2015) ;
- Données financières : CapitalIQ ;
- “Why Software Is Eating The World”, Marc Andreessen, Wall Street Journal (20/08/2011) ;
- “The Driverless Car, Officially, Is a Risk”, Wall Street Journal (3/3/2015) ;
- “Driverless cars could shrink motor insurance industry by 60 %”, The Actuary (19/6/2015) ;
- “Self-Driving Cars Could Cut Down on Accidents”, Wall Street Journal (5/03/2015) ;
- “Driverless Cars : Insurers Cannot be Asleep at the Wheel”, Bank Underground - blog des équipes de la Banque d’Angleterre (19/06/2015).

Les caractéristiques des futurs leaders de la cyber-assurance

- “Managing Cyber Risk and the Role of Insurance”, CSIS, (10/09/2015) – voir interventions de Suzanne Spaulding, Under Secretary, National Protection and Programs Directorate, Department of Homeland Security ;
- “Cyber Incident Data and Analysis Working Group White Papers”, Department of Homeland Security (2015) ;
- “Wearable tech & Health Insurance”, Forbes, (19/06/2014) ;
- “Wearable technology to transform health insurance industry” extrait de “Insight Report : Digital Innovation in Insurance”, Timetric (15/07/2015) ;
- “What if Fitness Wearables Affected Our Health Insurance Rates ?”, Varonis (12/3/2015) ;
- “The single biggest reason why startups succeed”, Bill Gross, TED (3/2015).

Annexes

Offre PwC sur la cyber-sécurité

Nous fournissons un large éventail de services intégrés dans le domaine de la cyber-sécurité qui vous aideront à évaluer, à développer et à gérer vos capacités en matière de cyber-sécurité, et à réagir face aux incidents et aux crises. Nos services sont conçus pour vous aider à renforcer la confiance, à comprendre les menaces auxquelles vous êtes confronté et vos vulnérabilités, et à sécuriser votre environnement. Notre équipe de spécialistes de la cyber-sécurité compte des experts dans les domaines suivants : réponses aux incidents, risques, gestion du changement, aspects juridiques et technologiques.

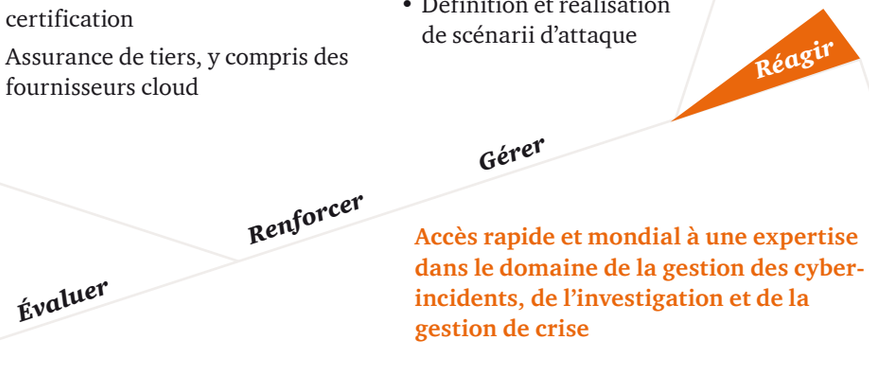
Comprendre vos capacités et votre niveau de maturité pour vous aider à hiérarchiser vos investissements

Cyberassurance

- Diagnostic de cybersécurité piloté par les cadres dirigeants
- Benchmark Cybersécurité
- Évaluation et modélisation des cybermenaces
- Exécution de programme d'audit intrusif interne et externe
- Revue des politiques de sécurité
- Conformité aux normes et certification
- Assurance de tiers, y compris des fournisseurs cloud

Cybermenaces

- Modélisation des menaces et des mécanismes d'alerte
- Exposition aux menaces persistantes avancées (APT - Advanced Persistent Threats)
- Intelligence sur les sources ouvertes
- Définition et réalisation de scénarii d'attaque



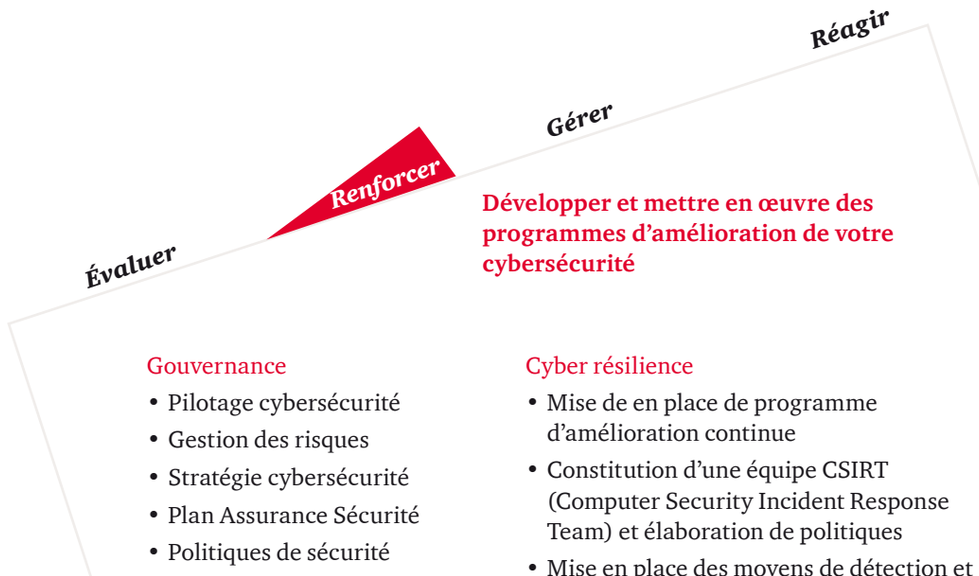
Accès rapide et mondial à une expertise dans le domaine de la gestion des cyber-incidents, de l'investigation et de la gestion de crise

Forensic

- Investigation sur les traces d'activité (applications, ordinateurs et réseaux)
- Analyse malware
- Investigation face à un cyberincident identifié
- e-Discovery et mise en évidence
- Analyse post-mortem

Fraude

- Analyse des données sur les fraudes et les cybercrimes
- Détection et mise en quarantaine des intrusions
- Identification des schémas des fraudes
- Prévention de la fraude



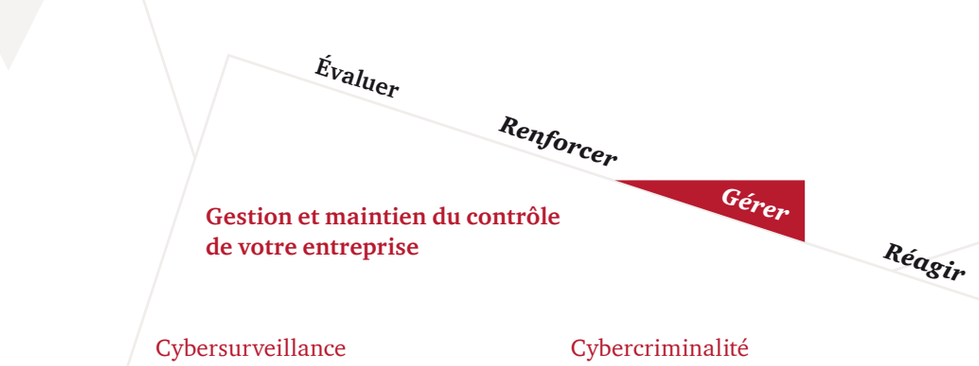
Développer et mettre en œuvre des programmes d'amélioration de votre cybersécurité

Gouvernance

- Pilotage cybersécurité
- Gestion des risques
- Stratégie cybersécurité
- Plan Assurance Sécurité
- Politiques de sécurité
- Sensibilisation et formation

Cyber résilience

- Mise de en place de programme d'amélioration continue
- Constitution d'une équipe CSIRT (Computer Security Incident Response Team) et élaboration de politiques
- Mise en place des moyens de détection et réponse aux menaces
- Pilotage des contre-mesures et remédiations



Gestion et maintien du contrôle de votre entreprise

Cybersurveillance

- Détection et surveillance des menaces avancées
- Accompagnement au renforcement des capacités de cyberdéfense
- Surveillance des fuites de données
- Services intégrés de gestion de la sécurité
- Gestion des vulnérabilités
- Services de réponse aux incidents

Cybercriminalité

- Service persistant de gestion des alertes et réponse à incident
- Préservation de la preuve
- Préparation d'actions en justice
- Identification des schémas des fraudes
- Évaluation des préjudices

PwC le leader mondial en Conseil et en Audit

PwC met son réseau pluridisciplinaire international au service des entreprises et organisations françaises et internationales.

Nos métiers

- Audit et Commissariat aux comptes
- Conseil en stratégie et consulting
- Conseil en transactions
- Conseil juridique et fiscal
- Expertise comptable

PwC, un réseau mondial structuré au service de la qualité

PwC France est membre du réseau international PwC.
En adhérant au réseau PwC, chaque membre bénéficie d'une licence d'utilisation du nom PwC et a accès à des technologies et méthodologies d'audit, de formation et de gestion. En retour, il s'engage à se conformer aux règles et politiques communes au sein du réseau et à respecter des standards de qualité.
Notre organisation mondiale permet d'assurer la meilleure qualité de service à nos clients mondiaux et de proposer une exécution de nos missions identique dans l'ensemble du réseau et une mise en œuvre homogène de notre approche d'audit tout en conservant la proximité avec nos clients.
C'est le choix qu'a fait PwC, celui d'un équilibre subtil entre organisation de taille mondiale et organisation à taille humaine proche de ses clients.

PwC France

Notre maillage régional : un équilibre et une homogénéité uniques au sein des réseaux d'audit

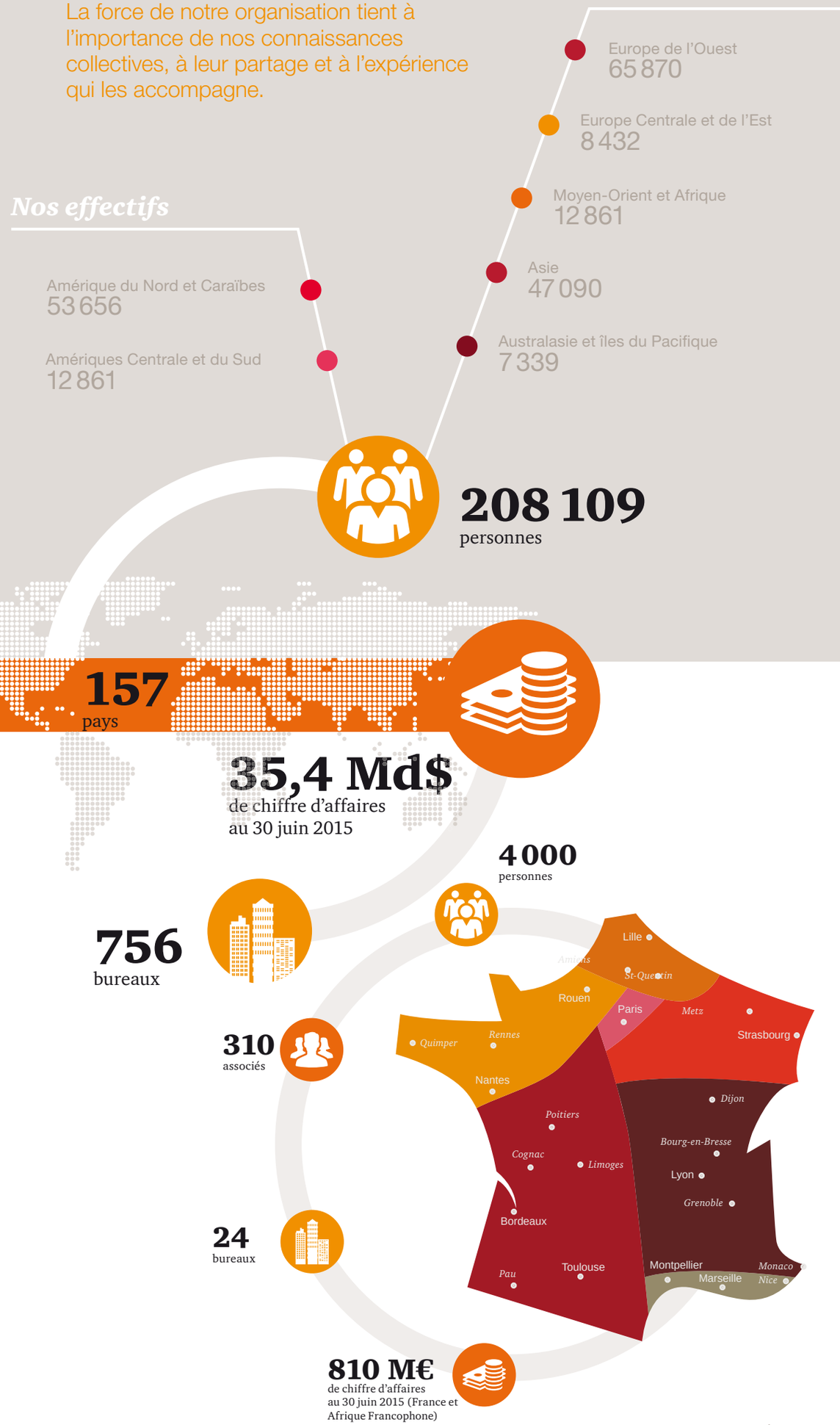
Partenaire essentiel de la vie économique locale dans 24 villes autour de 6 pôles de compétences régionaux en France, PwC accompagne l'ensemble des acteurs du secteur privé et du secteur public dans leur développement local, national et international, et ce depuis plus de 20 ans.

Intervenant sur l'ensemble des secteurs économiques des régions, nos équipes proposent une offre de services personnalisée et intégrée.

PwC fait ainsi bénéficier les acteurs régionaux de la force de son réseau international, porté par des structures de coordination et des méthodologies éprouvées, pour les accompagner dans leur développement.

La force de notre organisation tient à l'importance de nos connaissances collectives, à leur partage et à l'expérience qui les accompagne.

Nos effectifs



Notre expertise de premier plan dans le secteur de l'assurance

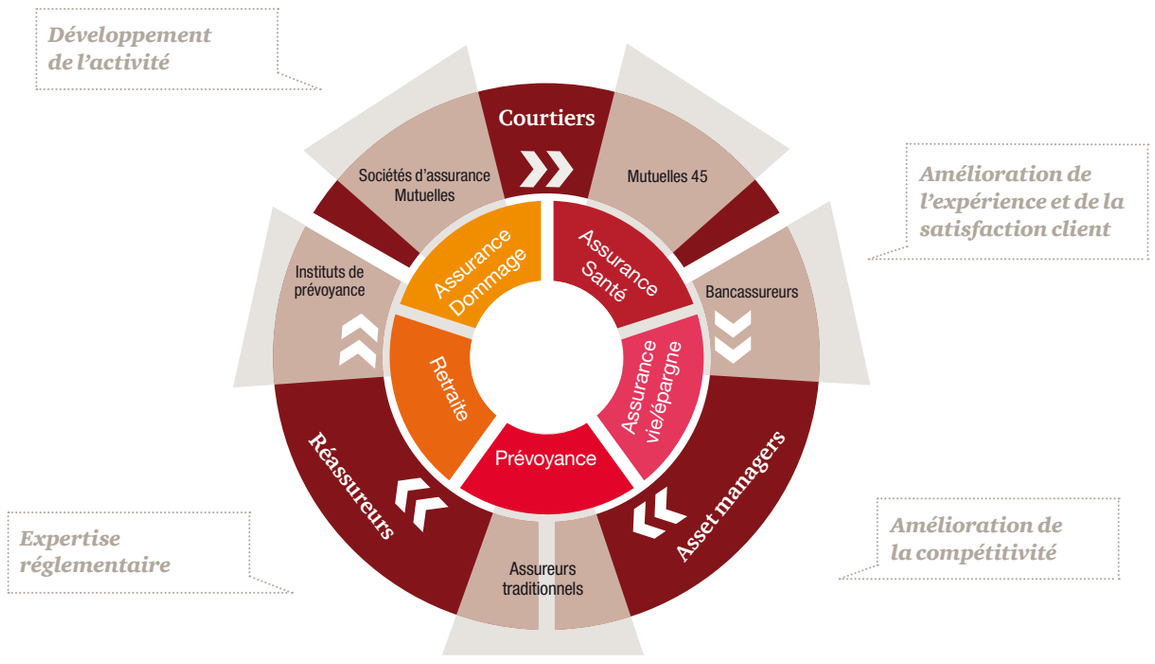
PwC est l'un des principaux cabinets de conseil en France, cumulant à la fois des compétences techniques fortes et une approche différenciée selon les entreprises.

PwC Conseil s'attache notamment à construire une relation dans la durée avec ses clients dans l'assurance, en les accompagnant à la fois en amont et en aval des missions. Fournissant des services à forte valeur ajoutée, grâce à une expérience acquise au fil des années, et s'impliquant totalement aux côtés des acteurs de l'assurance sur toute la durée de leurs projets, PwC Conseil intervient principalement autour de 4 problématiques :

- Développement de l'activité,
- Amélioration de la compétitivité,
- Amélioration de l'expérience et de la satisfaction client,
- Expertise réglementaire (Solvabilité II, IFRS4 - P2/IFRS9).

PwC est également l'un des principaux cabinets d'audit sur le marché de l'assurance et de l'économie sociale en France, avec des mandats portant notamment sur 6 des 10 principaux groupes présents dans notre pays (AXA, CNP Assurances, Crédit Agricole Assurances, Groupama, Covéa…) ainsi qu'un portefeuille significatif de mutuelles (Istya, MGEN, La Mutuelle Générale, MNCE), ce qui lui a permis d'acquérir une expérience forte sur les problématiques spécifiques de ce secteur.

Cette forte présence sur le marché et notre implication dans les instances professionnelles, normalisatrices ou réglementaires, nous a permis d'accompagner nos clients, dans le cadre de nos mandats légaux ou dans le cadre de missions de conseil, sur l'ensemble des projets et défis clés du secteur de l'assurance et de la mutualité. Cette expérience nous donne une large vision des pratiques de marché ainsi qu'un réel savoir-faire et contribue à sécuriser les décisions prises par les clients que nous accompagnons.



Les activités d'audit et de conseil de PwC en France et en Afrique francophone

PwC est aujourd'hui le seul cabinet capable d'accompagner ses clients « de la stratégie à l'exécution » pour améliorer la performance de nos clients et accompagner leur transformation en s'engageant sur la mise en place de solutions concrètes et opérationnelles.

Technology Consulting
- *Stratégie & Architecture*
- *Enterprise Applications*
- *Information Management*
- *Transformation fonction SI*
- *Sécurité & Infrastructure IT*

Ressources Humaines et Conduite du Changement
- *Transformation fonction RH*
- *Politiques et Processus RH*
- *Accompagnement RH de transformation • Gestion du changement et communication*
- *Gestion des Talents*

Finance Consulting
- *Finance Strategy • Finance & Accounting Operations*
- *Enterprise Performance Management • Corporate Treasury*

Strategy Consulting
- *Corporate Strategy • Sales and Marketing • Market & Customer Insights • Commercial and Operational deals services*

Transactions
- *Transactions Services*
- *Évaluation • Corporate Finance*
- *Financement de projets*

Litiges et Investigations
- *Litiges • Investigations • Forensic Technology Solutions*

Risk Assurance & Advisory Services
- *Gestion des risques et contrôle interne • Conformité • Data Assurance • Risques et Gouvernance IT • Services à l'audit interne*
- *Mesure des risques et de la valeur (finance, actuariat) • Protection sociale*

Capital Markets & Accounting Advisory Services

Conseil juridique et fiscal

PwC Société d'Avocats

500
personnes

- **Fiscalité internationale et droit des affaires international**
- **Prix de transfert**
- **Fusions et acquisitions**
- **Ressources Humaines**
- **Taxe sur la valeur ajoutée et droits indirects**
- **« Tax accounting »**
- **« Tax controversy & dispute resolution »**

Expertise comptable

600
personnes (dont 250 en île de France)

Des équipes pluridisciplinaires dédiées et structurées autour de 3 domaines de compétences pour servir tant des grands groupes ou des filiales étrangères que des ETI ou PME, en leur apportant des solutions à la carte : d'une assistance opérationnelle immédiate à l'externalisation complète.

Comptabilité et contrôle de gestion

- Renforcer votre service comptable et financier
- Apporter une expertise sur le traitement d'opérations comptables spécifiques
- Accompagner une transition comptable ou des projets spécifiques
- Prendre en charge toute ou partie de la production de vos comptes statutaires, reportings financiers ou obligations déclaratives
- Identifier des sources d'amélioration sur les aspects opérationnels comptables et partager les bonnes pratiques

Consolidation

- Assister vos équipes de manière ponctuelle ou récurrente dans la production des comptes consolidés ou de paliers de consolidation

Externalisation de la paie et gestion des RH

- Accompagner l'externalisation avec la dématérialisation des bulletins de paie ou de la signature des contrats de travail

Votre contact PwC

Pauline Adam-Kalfon
Directrice Assurance
PwC Consulting
Pauline.adam-kalfon@fr.pwc.com
https://fr.linkedin.com/in/paulineadamkalfon