RISQUE CYBER

COMMENT LES CABINETS DE COURTAGE DE PROXIMITÉ PEUVENT-ILS S'EN PRÉMUNIR ET CONSEILLER LEURS CLIENTS ?

INSTITUT INTERMEDIUS

PLANETE CSCA

LE SYNDICAT DES COURTIERS D'ASSURANCES

SOMMAIRE

PRÉAMBULE

INTERMÉDIUS, UN LABORATOIRE D'IDÉES

Créé à l'initiative de Bertrand de Surmont, Président de la Chambre Syndicale des Courtiers d'Assurances (aujourd'hui PLANETE CSCA), l'Institut Intermédius est une structure de réflexion prospective sur le secteur de l'intermédiation en assurances.

L'esprit qui anime ce think tank est d'associer à ses réflexions des personnalités de tous horizons, dans une volonté d'inter- professionnalité et d'échanges multisectoriels, vecteurs d'enrichissement des débats et de co-construction des préconisations.

Intermédius interroge régulièrement des personnalités qualifiées (courtiers, entrepreneurs, analystes, chercheurs, philosophes ...) tous spécialistes incontournables dans le domaine étudié.

Les travaux de l'Institut représentent un outil de doctrine pour la profession et s'inscrivent dans le cadre des différents débats publics. Ils ont vocation à être partagés avec chacun des acteurs de l'intermédiation (autorités de tutelle, régulateurs, élus, organisations professionnelles du secteur ..).

La numérisation de notre économie engendre de nouveaux risques pesant sur les entreprises connus sous le nom de « risques cyber ». De nombreux rapports en font le constat.

C'est pourquoi, cette année, l'Institut a choisi de mener ses travaux sur cette préoccupation majeure des entreprises, mais aussi des assurés. L'enjeu de cette réflexion sera de comprendre pourquoi et comment les cabinets d'intermédiation en assurance de proximité doivent-ils se protéger et, par capillarité, protéger leurs clients, afin de renforcer notamment la relation de confiance avec les assurés.

L'Institut Intermédius tient à remercier les différentes personnalités qualifiées qui ont contribué à cette cinquième édition :

Alain Bouillé
Délégué général du Club des Experts de la Sécurité de l'Information et du Numérique

Nicolas Bouzou
Économiste et essayiste

Christophe Delcamp
Direction des assurances de dommages et responsabilités de France Assureurs

Benoit Grouchko
Co-fondateur de DATTAK

Christophe Hautbourg
Directeur général de PLANETE CSCA

Laurent Devorsine
Président du Lab PLANETE CSCA

Lari Lehtonen
Responsable d'équipe Cyber Développement chez Marsch

Nathalie Malicet
Commissaire aux comptes et présidente de la commission numérique et innovation de la Compagnie nationale des commissaires aux comptes

Sébastien Meurant
Sénateur du Val d'Oise et co-rapporteur de la mission « La cybersécurité des entreprises »

Jules Veyrat
Co-fondateur de STOÏK

Laurent Perret
Directeur général d'EDICourtage

Jérôme Notin
Directeur général de Cybermalveillance

Laurent Arachtingi
Directeur général de l'IFPASS

Pascal Courthial
Senior Advisor Business Development Executive et Niamkey Ackable, expert en cyber resilience, Kyndryl France

Michèle Horner
Responsable relations courtiers pour la France
Luc Vignancour
Responsable Souscription Cyber, et
Jad Nehmé
Cyber Services et Client Expérience Manager - chez Beazley

Michael Monerau
PDF de la société QONTROL

Dorothée Decrop
Secrétaire générale HEXATRUST

PLANETE CSCA
LE SYNDICAT DES COURTIERS D'ASSURANCES

PLANETE CSCA, FONDATEUR D'INTERMÉDIUS

PLANETE CSCA est le seul syndicat représentatif du courtage d'assurances en France. Avec plus de 2 300 adhérents représentant les trois quarts des entreprises du secteur (en chiffres d'affaires), PLANETE CSCA s'appuie sur ses 9 collèges régionaux et de proximité et ses 6 collèges catégoriels pour fédérer toutes les typologies de cabinet de courtage en France.

CGPA
vivre votre profession avec assurance

CGPA, PARTENAIRE D'INTERMÉDIUS

CGPA est spécialisée dans les domaines de la Responsabilité Civile Professionnelle et de la Garantie Financière des Intermédiaires d'assurance depuis plus de 90 ans. CGPA accompagne ainsi 95% des agents généraux et plus de la moitié des courtiers français. Elle garantit aussi les activités des intermédiaires en transactions immobilières, des intermédiaires en opérations de banque, des conseillers en investissements financiers et des démarcheurs bancaires ou financiers.

LE MONDE DU COURTAGE EN 2023

UNE PROFESSION DYNAMIQUE

3,576 mrds €

Chiffre d'affaires des 50 plus grands cabinets généralistes français pour 2020 (+5,3% par rapport à 2018)

25 639

Courtiers d'assurances ou de réassurances en 2020 (contre 24 988 en 2018), soit un solde positif de +3 %.

10 532

Courtiers exercent l'activité à titre exclusif soit 41 % de l'ensemble des intermédiaires d'assurances enregistrés sur le Registre ORIAS.

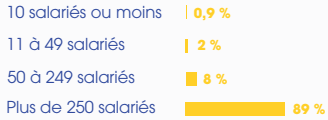
UNE FORTE MAJORITÉ D'ACTEURS DE PETITE TAILLE

89 %
des TPE
(moins de 11 salariés)

représentent

28 %
des emplois

RÉPARTITION DES ENTREPRISES SELON LA TAILLE



RÉPARTITION DES SALARIÉS SELON LA TAILLE DE L'ENTREPRISE

ÉDITO

NICOLAS BOUZOU,
ÉCONOMISTE & ESSAYISTE

Une étude réalisée par Asterès en 2022 a chiffré le coût des cyber attaques réussies en France à 2 milliards d'euros. Ce coût se répartit entre un coût direct de 887 millions d'euros, le paiement des rançons pour 888 millions d'euros et les pertes de production des entreprises et des services publics pour 252 millions d'euros. En 2022 toujours, Asterès estime que 385 000 attaques ont été réussies !

Pour les intermédiaires en assurance, cette nouvelle donne revêt deux dimensions. Les intermédiaires doivent se protéger, et protéger l'économie. Les cybercriminels perfectionnent continuellement leurs méthodes. Des ransomwares aux attaques par hameçonnage, aucun secteur n'est plus à l'abri. Se contenter de solutions de sécurité obsolètes ou basiques expose inévitablement l'entreprise à des risques accrus.

Le secteur de l'assurance, production ou distribution, ne peut s'affranchir de la confiance du public. Les clients confient leurs informations les plus sensibles aux courtiers en assurance, dans l'espoir d'obtenir une protection optimale contre les aléas de la vie. Les informations fournies par les clients lors de la souscription d'une assurance peuvent être sensibles. Elles incluent des données personnelles, financières ou liées à la santé. Une violation de ces données expose les intermédiaires a un risque réputation et à d'éventuelles poursuites judiciaires. Investir dans des systèmes de sécurité robustes est donc non seulement une question de conformité réglementaire, mais aussi de préservation de la confiance du client. Au-delà de la simple protection, une cyber-sécurité solide peut être un véritable atout commercial. Dans un monde où les violations de données font régulièrement les gros titres, un intermédiaire en assurance qui peut démontrer des mesures de sécurité exceptionnelles gagne en attractivité.

Les intermédiaires en assurance doivent se protéger contre le cyber-risque mais aussi proposer des protections à leurs clients. Comme le montrent les chiffres calculés par Asterès, les cyberattaques ne sont pas de simples scénarios catastrophes lointains. Elles font désormais partie de notre réalité quotidienne. Des grandes corporations aux PME, personne n'est à l'abri. Une cyberattaque réussie peut paralyser l'activité d'une entreprise pendant des jours, voire des semaines. Les coûts associés à cette interruption, combinés à ceux de la remédiation, peuvent être colossaux. Une assurance adaptée offre une bouée de sauvetage précieuse pour assurer la continuité d'activité. Avec la prise de conscience des risques liés au cyberespace, la plupart des pays ont renforcé leur cadre réglementaire. Des régulations comme le RGPD en Europe imposent des normes strictes en matière de protection des données et prévoient des sanctions en cas de manquement. Une assurance cyber-risque offre ainsi une double protection : contre la menace elle-même, mais aussi contre les conséquences d'une non-conformité.

De manière générale, les intermédiaires jouent un rôle de conseil. Ils doivent donc anticiper les besoins de leurs clients et les sensibiliser aux risques émergents. En mettant en avant des assurances dédiées au cyber-risque, ils affirment leur rôle de partenaire des entreprises. ●

DIAGNOSTIC, ENJEUX & DÉFIS

QUELQUES NOTIONS À CONNAITRE SUR LA CYBERSÉCURITÉ [1]

Attaque en déni de service
Attaque qui vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.

Cloud
Le cloud computing consiste à externaliser ses données informatiques vers des serveurs externes, distants.

Cybersécurité
État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Espiogiciel ou « spyware »
Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur les usages habituels des utilisateurs du système sur lequel il est installé, à l'insu du propriétaire et de l'utilisateur.

Fraude au président
Cette fraude consiste à récupérer indûment de l'argent devant être versé à un tiers légitime.

Malware
Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau.

Parefeu ou « firewall »
Outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet.

« Phishing » ou hammeçonnage «
Attaque reposant généralement sur une usurpation de l'identité de l'expéditeur.

« Ransomware » ou rançongiciel
Forme d'extorsion imposée par un code malveillant sur un utilisateur du système.

Spams
Tout courrier électronique non sollicité par le destinataire.

---

[1] *Source : site cybermalveillance.gouv.fr, ANSSI et CNIL.*

UN ENJEU MONDIAL QUI EXIGE UNE RÉPONSE COLLECTIVE

Il y a encore quelques années, le risque cyber n'était pas un sujet de préoccupation majeur. Aujourd'hui, sous l'effet d'une digitalisation, d'une interconnexion croissante des organisations et d'une menace généralisée, la tendance s'est inversée. Notre dépendance digitale accroit notre exposition au risque cyber et notre appréciation de l'importance de ce risque.
La cybercriminalité se fait de plus en plus menaçante. Le coût du risque cyber serait de 6 000 milliards de dollars, ce qui correspondrait à **la 3e économie mondiale[2].** Aujourd'hui, une cyberattaque peut cibler des **milliers d'entreprises** à la fois, n'importe où dans le monde.

Le baromètre des risques 2023 d'Allianz révèle – pour la 2e année consécutive - que, dans le monde, le risque cyber constitue dorénavant **la première préoccupation**, suivie des interruptions d'activités. Sont principalement en cause des attaques de rançongiciels combinées à des problèmes engendrés et accentués par la numérisation de notre société. En France, les incidents cyber sont répertoriés en **2e position** après les interruptions d'activités (liées notamment à des perturbations de la chaîne logistique)[3].

La profession de l'assurance et de la réassurance a réalisé sa sixième cartographie prospective 2023 des risques . Ce baromètre a été élaboré par la commission Analyse des risques de France Assureurs en interrogeant, fin 2022, les dirigeants de la profession.

À horizon 5 ans, les cyberattaques, le dérèglement climatique et l'environnement économique sont les trois principales menaces signalées par la profession. Ce risque occupe cette position depuis la première édition de la cartographie, même si son score recule légèrement, illustrant la mise en application dans les entreprises d'assurance et des grandes entreprises de mesures et protocoles stricts visant à renforcer la sécurité des systèmes d'informations.

---

[2] *La cyber sécurité des entreprises, rapport du Sénat, juin 2021*
[3] *Allianz Risk Barometer 2023*
[4] *France Assureurs*

LE RISQUE CYBER, PREMIÈRE PRÉOCCUPATION DES ENTREPRISES FRANÇAISES

The Global Risks Report, publié en 2022 à l'occasion du Forum économique de Davos, place à la **7e position** le risque cyber sur l'échelle des risques qui se sont aggravés depuis le début de la crise du Covid-19. Le rapport note également que les gouvernements font face à une montée de responsabilité à différents niveaux : sécurisation des infrastructures à risque, législation contre la cybercriminalité, sensibilisation de la population …
L'organisation mondiale alerte les gouvernements sur les attentes exigeantes des populations face à ce défi majeur.

Ces dernières années, les cybercriminels ont affiné leurs modèles économiques ainsi que leurs techniques ce qui rend les attaques plus faciles. Le Fonds monétaire international affirme que désormais « *les attaques informatiques pourraient aussi cibler des institutions financières d'importance systémique. En cas de succès, ces attaques pourraient entraîner une perte de confiance dans le système financier plus large, avec un impact potentiellement négatif sur la stabilité financière mondiale*[5] ». ●

Le développement du risque cyber est inévitable, il faut apprendre à vivre avec et s'adapter. Même si la majorité des attaques sont opportunistes et vise des entreprises détenant des informations personnelles « réutilisables »[6], tous les secteurs d'activités peuvent être impactés. En effet, des métiers plus « traditionnels » peuvent également être ciblés tout simplement parce que ces derniers ont recours à une plateforme de réservation en ligne ou traitent les factures via des échanges numériques[7].

[5] *Le Figaro, mai 2022*
[6] *Audition Jules Veyrat, 21 octobre 2022*
[7] *Audition Nathalie Malicet, 25 octobre 2022*

La numérisation de notre société, accélérée par l'adoption des nouveaux modes de travail, place la **cyber criminalité en tête des risques subis par les entreprises[8].** La peur d'être victime d'un acte de cybermalveillance reste forte : **44 % des dirigeants** interrogés disent craindre de perdre ou de se faire pirater des données[9]. En 2021, 54 % des entreprises françaises affirmaient avoir déjà fait l'objet d'une cyberattaque[10]. Et parmi elles, 60/65 % déposent le bilan dans les 18 mois[11].

Si **neuf entreprises françaises sur dix** estiment qu'il est essentiel de se prémunir contre les attaques informatiques, **une TPE-PME sur deux** ne sécurise pas ses postes de travail et **une sur trois** n'utilise même pas d'antivirus. Un décalage mis en lumière par une récente étude menée par l'Ifop[12]. En 2021, en France, **84 %** des grandes entreprises sont couvertes par une assurance cyber contre **0,3 %** des PME[13]. Un écart qui témoigne d'une prise de conscience très hétérogène face au risque cyber.

CONSTAT PAR LAURENT ARACHTINGI, DIRECTEUR GÉNÉRAL DE L'IFPASS

*« Le premier problème relatif à ce risque, c'est le problème de la **sensibilisation**. Pour exemple, j'échangeais récemment avec un Colonel de gendarmerie en charge des questions de cyber attaques, qui me disait que ¾ des collectivités ne sont pas couvertes, et 50 % n'ont même pas de référent sur le sujet ».*

« Ce qui m'interpelle, c'est qu'en 2023, il n'y ait pas une plus grande prise de conscience du risque de la part des dirigeants du privé comme du public ».

[8] *Rapport ANSSI 2021*
[9] *Le numérique dans les TPE-PME, France Num, septembre 2022*
[10] *Source baromètre de la cybersécurité en entreprise, CESIN 2022*
[11] *Audition Laurent Arachtingi, 13 mars 2023*
[12] *Rapport Ifop, les TPE/PME et la cybersécurité, décembre 2021*
[13] *AMRAE*

Afin d'apporter une réponse forte et coordonnée, adaptée aux réels besoins des entreprises, il convient avant tout de définir le terme de cyberespace. Dans son glossaire, l'ANSSI le définit comme un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisés de données numériques. Le gouvernement[14] ajoute qu'une cyber-attaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant. Elle cible différents dispositifs informatiques tels que les ordinateurs, les serveurs, les équipements périphériques (imprimantes) ou encore des appareils communicants (téléphones). Il existe principalement quatre types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage et le sabotage.

La réponse à ce nouveau risque passe par diverses solutions, certaines générales, d'autres plus spécifiques, qui peuvent être mises en œuvre concomitamment. Chaque entreprise doit y travailler à son propre niveau mais l'intérêt général commande d'adopter des mesures incitatives qui permettront de protéger l'économie nationale et de préserver autant que possible l'activité économique. La notation ESG (environnement, société, gouvernance) comporte d'ailleurs une référence à la cybersécurité qui constitue une dimension essentielle de la gouvernance de l'entreprise mais également de la responsabilité sociétale des entreprises sous l'angle notamment de la protection contre le vol des données[15]. Une formation sur le risque cyber peut être perçue comme un effort collectif, un vrai projet d'entreprise sur lequel la gouvernance peut communiquer[16].

Selon la dernière étude de l'Ifop et de l'entreprise Terranova Security[17], **62 % des Français** n'ont jamais reçu une formation à la cyber sécurité. Pour les personnes n'ayant jamais participé à des formations de sensibilisation la raison majeure réside, pour 53 %, dans le simple fait qu'ils ne se sont pas vu offrir des formations de ce type. L'intérêt des salariés, pourtant, est indéniable : 79 % estiment intéressante la formation en sensibilisation, même si leur entreprise ne la propose pas.

The Global Risks Report[18] note que **95 %** des problèmes de cybersécurité seraient imputables à une erreur humaine. Afin de sensibiliser le plus grand nombre, il apparait judicieux de dédramatiser le sujet et de le présenter de manière très pédagogique[19] .

---

[14] *Site cybermalveillance.gouv.fr*
[15] *Plateforme RSE, avis du mois d'avril 2021 - responsabilité numérique des entreprises*
[16] *Audition Nathalie Malicet, 25 octobre 2022*
[17] *De la protection des données à la culture cyber, Ipsos Terranova Security, octobre 2022*
[18] *Forum économique de Davos, 2022*
[19] *De la protection des données à la culture cyber, Ipsos Terranova Security, octobre 2022*

Face à ces sujets, les entités souffrent avant tout, d'une déficience humaines. Avant d'envisager une totale transformation numérique, il est nécessaire de « transformer », sensibiliser, former les hommes.
Pour se protéger efficacement, le coût peut représenter un à deux jour(s) de chiffre d'affaires de l'entreprise. Il s'agit d'un enjeu financier assez faible quand on sait qu'un dirigeant peut perdre son entreprise en 2 jours à cause d'une cyber attaque[20].

Récemment l'ANSSI, la CPME ou encore cybermalveillance.gouv.fr ont publié un guide des bonnes pratiques à destination des TPE-PME[21] leur livrant ainsi les treize règles essentielles pour sécuriser leurs informations. D'autres institutions concluent des partenariats avec des instances judiciaires, policières et consulaire (CCI) afin de sensibiliser les responsables de TPE-PME qui pensent passer sous le radar des crimes perpétrés par internet[22].

L'EXEMPLE À SUIVRE : CYBERAUDIT

La Compagnie nationale des commissaires aux comptes a élaboré un outil permettant de sensibiliser les TPE-PME aux risques cyber. Les réponses au questionnaire de 70 questions permettent aux commissaires aux comptes, en tant que tiers de confiance, d'élaborer un diagnostic afin de mettre en lumière les impacts financiers que pourrait avoir une attaque cyber au sein d'une entreprise.
Un tel diagnostic permet également aux commissaires aux comptes de tester leurs connaissances sur la thématique cyber.

« *L'esprit de cet outil est de permettre au commissaire aux comptes de sensibiliser son client sur les conséquences financières des différentes menaces qui peuvent peser sur son système d'information* ».

Nathalie Malicet
présidente de la commission numérique et innovation de la CNCC

[20] *Audition Laurent Arachtingi, 13 mars 2023*
[21] *https://www.ssi.gouv.fr/uploads/2021/02/anssi-guide-tpe_pme.pdf*
[22] *Audition Nathalie Malicet, 25 octobre 2022*

Il y a peu, les insurtechs DATTAK et STOÏK se sont lancées sur le marché en vue d'aider les TPE-PME, grâce à la technologie, à diminuer leurs risques cyber[23] . Leur mission : protéger des cyber attaques et les assurer. Pour cela, ils ont imaginé, en complément du volet assurantiel, des technologies de prévention du risque. Si l'on considère que chaque utilisateur d'un outil numérique peut être potentiellement le maillon faible au sein d'une entreprise, la réponse à apporter au risque cyber ne doit donc pas se limiter à l'aspect technologique mais doit aussi être apportée au niveau de la gouvernance et des salariés à travers une sensibilisation aux bonnes pratiques[24] . C'est en ce sens que DATTAK et STOÏK proposent des campagnes de formation sous forme par exemple de phishing personnalisés.

PAROLE D'EXPERT
BENOIT GROUCHKO, CO-FONDATEUR DE DATTAK[25]

La souscription d'un produit d'assurance pour les TPE-PME peut être soumise à certaines frictions. Afin de proposer la meilleure couverture assurantielle, il convient d'identifier avec précision les potentielles menaces notamment à l'aide d'un questionnaire de sécurité. Une méconnaissance ou une sous-estimation du risque par les entreprises peut engendrer un refus d'accompagnement de la part assureurs. Pour répondre à ces difficultés de souscription, DATTAK a développé un outil d'évaluation automatique du risque cyber de l'entreprise, mis à disposition des courtiers en assurance : en moins de deux minutes, un profil de risque est dressé. Cet outil n'implique pas nécessairement une proposition officielle de couverture du risque néanmoins cela permet de proposer un produit d'assurance adapté à un tarif compétitif en tenant compte de la probabilité de la survenance du risque.

[23] *Audition Benoit Grouchko, 26 octobre 2022*
[24] *Audition Nathalie Malicet, 25 octobre 2022*
[25] *Audition Benoit Grouchko, 26 octobre 2022*

Ces campagnes de sensibilisation poursuivent deux objectifs majeurs pour les intermédiaires en assurance : leur apprendre à appréhender le risque afin qu'ils puissent, à leur tour, éduquer leurs clients. Grâce à leur capacité à comprendre et à évaluer les risques, les courtiers aident leurs clients à identifier et souscrire des contrats d'assurances adaptés à leurs besoins. Le risque cyber étant aujourd'hui le premier risque pour les entreprises, il parait primordial de le maitriser afin de pouvoir assurer correctement ses clients. ●

LA STRATÉGIE FRANÇAISE FACE À LA MENACE

Le dernier baromètre de la cybertech Anozr Way[26] confirme que le niveau de la menace cyber n'a jamais été aussi critique. Selon l'étude, la perte de chiffres d'affaires cumulés pour les entreprises françaises, victimes de rançongiciel, s'élevait à **1,06 milliard d'euros** pour la période janvier-août 2022. En 8 mois, le nombre d'organisations qui ont été frappées par ce type d'attaque est déjà égal à 85 % de l'ensemble de l'année 2021, selon le même baromètre daté de septembre.

Dans son rapport en date de septembre 2022, la Direction générale du Trésor reconnait que la lutte contre le risque cyber constitue un enjeu majeur de souveraineté[27] . En effet, avant d'être un enjeu technologique, le risque cyber représente un enjeu sociétal et économique. L'endurance et la fiabilité des infrastructures ainsi que des logiciels sont fondamentales pour la conduite des affaires publiques, l'activité des entreprises, la sécurité des données personnelles des utilisateurs et le fonctionnement même des institutions[28] . L'État qui ne ferait pas de son mieux pour les garantir s'exposerait à des menaces graves et à la défiance de ses citoyens. C'est pourquoi, il est urgent de mener une forte sensibilisation permettant d'atteindre l'objectif ultime : être en mesure de détecter une attaque le plus rapidement possible afin de limiter l'impact financier et permettre à l'entreprise de reprendre son activité rapidement[29] .

À l'occasion de la Stratégie nationale pour la sécurité du numérique de 2015, l'état est à l'époque parti du constat que, s'il était plutôt en mesure de protéger ses propres infrastructures ou les infrastructures vitales du pays, il se devait d'apporter une réponse structurée aux autres composantes de la société, souvent désarmées face à une cybercriminalité en plein essor.

---

[26] *Baromètre du Ransomware, septembre 2022*
[27] *Rapport DG Trésor, Le développement de l'assurance du risque cyber, septembre 2022*
[28] *Le cyber, enjeu de souveraineté, La Croix, décembre 2020*
[29] *Audition Nathalie Malicet, 25 octobre 2022*

C'est de cette volonté qu'est né, en mars 2017, le GIP ACYMA[30], qui a piloté, en octobre 2017, l'ouverture de la plateforme **Cybermalveillance.gouv.fr** : le dispositif national de sensibilisation, prévention et d'assistance aux victimes d'actes de cybermalveillance pour les particuliers, entreprises et collectivités territoriales (hors Opérateurs d'Importance Vitale et Opérateurs de Services Essentiels).

Un dispositif original porté par un partenariat public privé et qui regroupe des acteurs étatiques impliqués tels que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) des services du Premier ministre, le ministère de l'Intérieur, le ministère de la Justice, le ministère de l'Économie et des Finances, le secrétariat d'État en charge du Numérique et le ministère des Armées. À leurs côtés sont également rassemblés de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des éditeurs…

Les missions du GIP sont de lutter contre les actes de cybermalveillance, en se basant sur une stratégie d'action articulée autour de trois axes clés :

1

Assister les victimes d'actes de cybermalveillance grâce à la plateforme Cybermalveillance.gouv.fr, qui assure un service d'assistance en ligne aux victimes et une mise en relation avec des professionnels en cybersécurité référencés.

2

Prévenir les risques et sensibiliser sur la cybersécurité avec la réalisation de **publications et de campagnes de sensibilisation et de prévention contre les cybermenaces, grâce à des contenus sous différents formats (vidéos, fiches, kit de sensibilisation, affiches, stickers, mémos…) et à travers l'accompagnement à la sécurisation des systèmes d'information des publics professionnels** (entreprises, collectivités et associations) par des prestataires labellisés ExpertCyber.

3

Observer et anticiper le risque numérique grâce à la remontée et l'analyse de données d'utilisation, qui permet d'accroitre la connaissance de la menace numérique et ainsi adapter les actions d'assistance et de sensibilisation du dispositif Cybermalveillance.gouv.fr.

En complément de l'indispensable sensibilisation/information, et dans une démarche d'amélioration du niveau des professionnels en cybersécurité, un label de qualité sur l'expertise numérique[31] a été développé en partenariat avec les principaux syndicats professionnels du secteur et le soutien de l'AFNOR.
Il vise à reconnaître l'expertise des experts en cybersécurité assurant des prestations d'installation, de maintenance et d'assistance en cas d'incident.

Les prestataires labellisés ExpertCyber s'adressent à un public professionnel. **Faire appel à un prestataire labellisé garantit aux bénéficiaires un accompagnement de qualité.**

À l'heure où une nouvelle étude pointe du doigt le retard de la France en matière de « cyber culture »[32], le gouvernement français renforce ses ambitions afin de se prémunir des attaques informatiques.

En février 2021, Cédric O a annoncé l'attribution d'une enveloppe d'**un milliard d'euros**, dont 720 millions de financement public au secteur de la cybersécurité. Cette stratégie nationale s'inscrit dans le plan d'investissement France 2030 et a pour objectif de **tripler le chiffre d'affaires du secteur cyber et créer 37 000 emplois d'ici 2050.** Une feuille de route confirmée récemment par le ministre délégué à la transition numérique, Jean-Noël Barrot, qui a aussi alerté sur la pénurie de talents. À l'occasion de sa visite du Campus Cyber le 28 octobre 2022, le ministre annonce un soutien à hauteur de **39 millions d'euros** à 17 projets d'envergure pour hisser la France au rang des champions mondiaux de la cybersécurité[33]. Ces projets visent à contribuer au développement de solutions innovantes en cybersécurité, à renforcer les dynamiques collaboratives entre les acteurs de l'écosystème et à accroitre l'offre de formation en cybersécurité.

Les objectifs, à court terme, de la stratégie française sont : augmenter le chiffre d'affaires de la filière à **25 milliards d'euros** en 2025 (contre 7,3 en 2019), positionner la France par rapport à la concurrence internationale en doublant notamment les emplois de la filière pour passer à **75 000** en 2025 (contre 37 000 aujourd'hui) ou encore diffuser une véritable culture de la cybersécurité dans les entreprises et notamment les plus petites d'entre elles afin de leur permettre d'optimiser la sécurité de leurs réseaux[34].

---

[31] *Audition Jérôme Notin, 9 mars 2023*
[32] *De la protection des données à la culture cyber, Ipsos Terranova Security, octobre 2022*
[33] *Communiqué de presse, 28 octobre 2022*
[34] *Site de l'ANSSI*

Si la cybersécurité représente une menace pour les entreprises, elle constitue également une opportunité de développer un marché porteur. Toutes les entreprises étant exposées, le risque cyber ne va cesser de se développer et de créer des emplois, dans un monde numérique de plus en plus étendu[35] . Pourtant la pénurie de talents en matière de cyber sécurité est mondiale[36]. Le Sénat affirme dans son rapport que **70 %** des entreprises dans le monde manquent de spécialistes en sécurité informatique et qu'il faudrait en former.**4 millions** pour répondre aux besoins du marché. Un handicap particulièrement aggravé pour les TPE-PME pour lesquelles la ressource humaine devient pratiquement inaccessible.

Inauguré en février 2022, le Campus Cyber incarne la politique française en matière de cybersécurité. Rassemblant plus de **160 acteurs nationaux et internationaux** de la sécurité numérique, ce campus permet de favoriser la réalisation de projets de recherche et de développement ainsi que l'éclosion des licornes cyber de demain. À terme, le gouvernement espère que ce Campus permettra de donner naissance à des champions français du secteur, à échelle mondiale.

Car en effet, « en termes de cybersécurité, la France est en net retrait par rapport aux pays anglo-saxons, que ce soit au niveau de la formation, des gestes ou du niveau de compétence perçu. Cela peut s'expliquer par une part de télétravail plus faible et, par extension, une exposition moindre aux risques. La perception des menaces reste néanmoins élevée, soulignant un enjeu fort de pédagogie en termes de cybersécurité. », constate ainsi Anselme Laubier, directeur d'études chez IPSOS.

Également, la loi du 3 mars 2022 a instauré la mise en place d'un « cyber-score » et qui deviendra obligatoire le 1er octobre 2023 (applicable dans un premier temps à tous les grands opérateurs du numérique pour le public). Le Cyber Score est une méthodologie qui permet aux entreprises de mesurer leur maturité et leur niveau de risque en matière de cybersécurité.

[35] Audition Benoit Grouchko, 26 octobre 2022
[36] Audition Benoit Grouchko, 26 octobre 2022

Il vise la transparence et la responsabilité, et à :

- Informer sur le niveau de sécurité du prestataire et de la solution ;
- Favoriser l'achat auprès de fournisseurs sécurisés et « responsables » ;
- Lier la cybersécurité à la responsabilité sociétale de l'entreprise.

L'obtention du « Cyber-Score » se fera après audit de cybersécurité par des prestataires d'audit agréées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Cet audit portera sur les données qu'ils hébergent directement ou par l'intermédiaire d'un tiers et visera :

- La sécurisation des données : recours au chiffrement, à l'anonymisation, etc… ;
- La localisation de l'hébergement : un facteur particulièrement critique puisque 90 % des données françaises seraient hébergées sur des serveurs états-uniens ;
- Et leur propre sécurisation.

Le 25 janvier 2023, la loi LOPMI (**Loi d'Orientation et de Programmation du ministère de l'Intérieur**) a été publiée[37]. Elle contient un article 5 qui crée dans le code des assurances un nouveau chapitre sur l'assurance des risques de cyberattaques avec un article unique qui fixe le régime juridique applicable à l'assurance des cyberattaques. **Depuis le 25 avril 2023**, les assurés (personnes morales et personnes physiques dans le cadre de leur activité professionnelle) sont dans l'obligation, pour pouvoir être garantis, de porter plainte auprès des autorités compétentes, au plus tard soixante-douze heures après la connaissance de la cyberattaque. Cette obligation pour les assurés de porter plainte concerne toutes les cyberattaques, y compris les attaques avec demande de rançon. S'agissant des modalités de dépôt de plainte, la LOPMI a également prévu qu'à partir de 2023, l'application mobile commune à la police et à la gendarmerie « Ma sécurité »[38] permette aux victimes (non spécifiques aux cyberattaques) de déposer plainte en ligne. Le délai de 72 heures pour porter plainte a pour avantage de correspondre au délai de 72 heures imposé par ailleurs aux responsables de traitement par la CNIL pour notifier une violation de donnée à caractère personnel à l'occasion notamment d'une cyberattaque.

Lors du Conseil des Ministres du 10 mai[39], le ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique et le ministre délégué auprès du ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique, chargé de la Transition numérique et des Télécommunications ont présenté le **projet de loi visant à sécuriser et réguler l'espace numérique** (SREN) pour restaurer la confiance nécessaire au succès de la transition numérique.

[37] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768
[38] https://www.interieur.gouv.fr/actualites/actu-du-ministere/lapplication-ma-securite-pour-faciliter-echanges-avec-gendarmerie-et
[38] Site du gouvernement

Les désordres dans l'espace numérique touchent les Français dans de nombreuses dimensions de leur vie quotidienne. Ce projet de loi présente des mesures concrètes **visant à renforcer l'ordre public et réguler l'espace** numérique, et ainsi assurer la confiance indispensable au succès de la transition numérique. Le moment est venu de **faire respecter les droits et les devoirs, et de garantir à chacun la cybersécurité du quotidien.** C'est ainsi que la France tiendra son rang de grande nation numérique.

Issu d'un travail interministériel mené par M. Jean-Noël BARROT, ce projet de loi contient une vingtaine de propositions. Il propose notamment de **protéger les Français contre les tentatives d'accès frauduleux à leurs coordonnées personnelles ou bancaires** à des fins malveillantes qui se sont multipliées ces dernières années.

Mais également, de manière plus générale, renforcer les sanctions des personnes condamnées pour cyberharcèlement, mieux protéger les enfants, sanctionner les sites en cas de non-retrait de contenus pédopornographiques en ligne, restaurer l'équité commerciale sur le marché du cloud, aujourd'hui concentré dans les mains d'une poignée d'acteurs, apporter des protections nouvelles contre la désinformation et les ingérences étrangères provoquées par la diffusion de médias frappés par des sanctions internationales.

Ce projet de loi trouve ses origines dans la nécessité d'adapter le droit pour que puissent s'appliquer **trois règlements européens que la France** a fait adopter lors de sa présidence de l'Union européenne en 2022 : **le règlement sur les services numériques (DSA)** qui fait entrer les grandes plateformes dans l'ère de la responsabilité, le règlement sur les marchés numériques (DMA) qui vient quant à lui rétablir l'équité commerciale dans l'économie numérique et enfin le Règlement sur la gouvernance des données (DGA), qui stimulera l'économie de la donnée européenne.

Alors qu'à Bruxelles, les outils de contrôle des géants du numérique prévus par les deux règlements DSA et DMA se mettent en place. Les premières tensions apparaissent avec certaines plateformes, accusées de ne pas respecter leurs obligations.

La première mesure créer un filtre de cybersécurité anti-arnaque. Demain, au moment de cliquer sur un lien après avoir reçu un SMS ou un mail frauduleux, un message d'alerte avertira les Français indiquant que le site vers lequel il se dirige est compromis. ●

LE RÈGLEMENT EUROPÉEN

Au niveau européen, **le Conseil a adopté le règlement sur la résilience opérationnelle numérique du secteur financier** (règlement « Digital Operational Resilience Act » - DORA), **qui doit permettre au secteur financier européen de rester résilient en cas de perturbation opérationnelle grave** (Publication au JOUE du 27/12/2022[40]).

Ce règlement d'application directe dans les États membres vise à imposer des exigences uniformes relatives à la sécurité des réseaux et des systèmes d'information sous-tendant les processus opérationnels des entités financières. Ce texte sectoriel s'appliquera, entre autres, aux intermédiaires d'assurance et de réassurance qui sont des personnes morales qui emploient plus de 250 personnes et dont le chiffre d'affaire annuel excède 50 millions d'euros; ce champ d'application réduit aux plus gros cabinets de courtage a été obtenu grâce à l'action conjointe de PLANETE CSCA et du BIPAR.

Le règlement repose sur 5 piliers :

- La mise en place d'un cCadre de gestion des risques informatiques qui soit solide, complet et documenté.
- Un reporting obligatoire à l'ACPR des incidents informatiques.
- La mise en œuvre d'un programme de tests de résilience opérationnelle (tests annuels et pour certains des tests d'intrusion fondés sur la menace).
- La mise en place d'un cadre de gestion du risque présenté par les fournisseurs tiers de services informatiques.
- La possibilité d'organiser entre entités financières des dispositifs de partage d'informations et de renseignements sur les cybermenaces.

Le Règlement prévoit également un nouveau cadre de surveillance pour les fournisseurs tiers critiques de services informatiques, comme les fournisseurs de cloud, qui seront « supervisés » par l'autorité européenne des assurances et des pensions professionnelles (EIOPA) qui veillera à ce que le niveau de sécurité et de disponibilité des services soit suffisamment élevé.

Ce règlement entrera en application le **17 janvier 2025** permettant ainsi à la Commission européenne, aidée par les autorités de contrôle européennes EIOPA, EBA et ESMA, de publier les actes délégués qui viendront préciser certaines exigences de DORA (niveau I) et constitueront le niveau II de cette nouvelle réglementation visant à renforcer la cybersécurité des entités financières européennes.

[40] *https://eur-lex.europa.eu/legal-content/FR/TXT*

Également, présenté par la Commission européenne en septembre 2022, le CRA (Cyber Resilience Act) **vise à « renforcer les règles de cybersécurité pour garantir des produits matériels et logiciels plus sûrs ».** Elle doit imposer des obligations de cybersécurité pour les produits et services numériques dans l'Union européenne mais elle pourrait avoir des conséquences pour les logiciels open source, selon des dirigeants de la communauté open source[41]. ●

LA NOTION DE CYBER RÉSILIENCE

L'évolution du paysage des risques de sécurité et l'industrialisation des cyberattaques ont entraîné un nombre croissant d'incidents de sécurité, la motivation liée aux gains avec un « retour sur investissement » rapides générés par les rançons ont transformé nos systèmes d'information en « cash-machine », des organisations cybercriminelles.

Les approches de sécurité conventionnelles ne sont plus suffisantes pour prévenir et contenir toutes les failles de sécurité des entreprises ou organisations, d'où la nécessité de repenser le modèle de protection en intégrant dans leur stratégie de sécurité, des mesures de résilience opérationnelle.

La résilience des systèmes d'information désigne la capacité d'un système ou d'un réseau informatique à continuer de fonctionner de manière normale en cas d'incident (panne, sinistre, pic d'activité, cyberattaque, etc.), et/ou à retrouver son état de fonctionnement initial le plus rapidement possible, avec le minimum d'effets indésirables.

La résilience opérationnelle ne doit pas être uniquement la préoccupation de spécialistes de l'informatique mais de l'ensemble des parties prenantes de l'entreprise, car il est impératif d'avoir une vision globale et cohérente de l'impact de l'exploitation des vulnérabilités et des failles sur l'entreprise.

Il s'agit « plutôt repartir du «Minimum Viable Company» (MVC) – c'est-à-dire la définition des processus, fonctions et services essentiels, voire vitaux, d'une entreprise – et (se) demander comment l'ensemble du système d'information peut les soutenir ».

Niamkey Ackable
Partner consult chez Kyndryl France[42].

[41] *Le CNLL (Union des entreprises du logiciel libre et du numérique ouvert) et d'autres organisations dont l'APELL - Association Professionnelle Européenne du Logiciel Libre*
[42] *Audition du 30 mai 2023*

Dans ce changement d'approche, il convient de bien comprendre ce qui constitue ce MVC pour une entité. Comprendre quels sont les systèmes et infrastructures en support de ces activités (ce que beaucoup d'entreprises omettent), et enfin tester quel serait l'impact de chaque vulnérabilité ou faille sur l'ensemble de l'organisation (ce que beaucoup d'entreprises ne font pas encore). Au plus haut niveau, une vision holistique de la résilience devient primordiale. Seule cette vue d'ensemble permettra d'identifier ce qui est réellement essentiel, voire vital.

La cyber résilience est la réponse pragmatique à l'évolution des enjeux liés à la fois à l'accélération de la transformation digitale et de la menace cyber, croissante et protéiforme qui pèse sur nos entreprises.

L'entreprise Kyndryl, leader en cyber résilience, est spécialisée dans les services d'infrastructure et d'infogérance autour de solutions de Cloud, de résilience et des services réseau pour aider à optimiser la transformation numérique des entreprises et protéger le parc informatique avec un niveau de sécurité et de résilience irréprochable.

Kyndryl ne propose pas uniquement des outils mais un service complet, de la conception d'un système propre, une méthode personnalisée, un suivi adapté à la taille et aux contraintes de l'entreprise. ●

PASCAL COURTHIAL, SENIOR ADVISOR BUSINESS DEVELOPMENT EXECUTIVE CHEZ KYNDRYL FRANCE[43]

La relation client-entreprise a évolué. « Ce n'est plus l'instant de l'achat qui compte, mais l'expérience client permanente. Dans le monde de l'assurance où tout est « digitalisable », faire la différence dans ce contexte impose une relation client sans couture ». La confiance, notamment, passe par la sécurisation des données.
Aujourd'hui, la sensibilisation et la vulgarisation ne suffisent plus, il fait prendre des mesures de sécurité préventives complexes, qui « ralentissent » l'attaquant, qui doit aller vite pour ne pas être démasquer.

L'idée est de ne plus fonctionner de façon artisanale, chaque entreprise de son côté, mais plutôt d'imaginer une « solution industrielle » commune (un socle commun) traduite par des démarches individuelles, avec un service personnalisé à géométrie variable selon la taille de l'entreprise, les enjeux des clients...

[43] *Audition du 30 mai 2023*

LES INTERMÉDIAIRES EN ASSURANCES ET LE RISQUE CYBER

Identifié comme un acte malveillant, une attaque cyber peut entrainer un arrêt brutal d'une activité professionnelle d'un grand groupe tout comme d'une TPE-PME. Les cabinets de proximité pensent encore, à tort, que seules les grandes entreprises sont touchées[44]. Nous sommes aujourd'hui face à une masse de TPE-PME qui, ne se méfiant pas, représentent des cibles faciles à atteindre et font l'objet d'attaques pouvant mettre en péril leur survie.

La majorité des cabinets de courtage en assurance sont majoritairement des TPE-PME (**89 %**) et conseillent eux-mêmes des entreprises parfois vulnérables.

La digitalisation des cabinets peut devenir extrêmement utile aux courtiers de demain notamment en matière de collecte de données personnelles[45]. Mais cette interconnexion croissante des systèmes d'information augmente les cyber risques.

Les cabinets d'intermédiation en assurance sont particulièrement concernés par le risque cyber par leur position de point d'entrée dans la chaîne de valeur de l'assurance. Ils peuvent être considérés comme une cible privilégiée notamment à cause de leur activité :

- Ils ont accès à des données sensibles très confidentielles et personnelles
- L'outil informatique est vital pour leur activité
- Ils gèrent des flux de trésorerie importants (prime, reversement ..)[46]

Les cabinets de courtage sont très dépendants de leurs systèmes d'information, la paralysie de celui-ci peut compromettre leur activité et leur existence à court terme.

Selon le Directeur de l'Ifpass[47] , la protection du risque cyber passe par :

- la **sensibilisation** des cabinets et de leurs clients
- la **prévention**, un rôle essentiel de l'assurance, en sensibilisant notamment les chefs d'entreprise à la mise en place d'un plan de continuité d'activité (PCA)
- la **formation**, des équipes en place (dirigeantes, salariés) ou des futurs professionnels du risque cyber.

[44] *Audition Jules Veyrat, 21 octobre 2022*
[45] *Intermédius, 2018 - IA et intermédation*
[46] *Audition Benoit Grouchko, 26 octobre 2022*
[47] *Audition Laurent Arachtingi, 13 mars 2023*

Conscient de ce risque pour la profession, le Groupe Ifpass, institut de référence de la formation, de l'emploi et des services dans les secteurs Assurance, Banque et Finance, a créée en 2022, en collaboration avec Jedha, des formations en data science et cybersécurité du niveau 4 (Bac) au niveau 7 (Bac+5), dans les secteurs de l'assurance, de la banque et de la finance.

Au printemps 2020, PLANETE CSCA a mis en place son Lab', identifiant plusieurs thématiques dont les systèmes d'information, la communication, ou le risque cyber …
Le Lab a pour objectif de répondre à des problématiques opérationnelles des courtiers en assurances.

Une fois les recommandations définies, le Lab pourra s'en saisir et les mettre en œuvre.

Laurent Devorsine , Président du Lab', alerte sur deux points majeurs, la formation et la relation avec les prestataires.

La profession n'est pas tout à fait au point d'autant plus que l'adhérent « type » de PLANETE CSCA est issu d'un cabinet de proximité qui emploie moins de 5 collaborateurs. Ceux-là ont une maturité digitale faible et ne sont pas au niveau en matière de sécurité informatique.
Il n'existe pas de statistique sur la sinistralité observée au sein de la branche. En effet, lorsqu'un cabinet de courtage se fait hacker, il a tendance à ne pas en parler.

> *« Je suggère d'intégrer le cyber dans le cadre de la formation digitalisée obligatoire (via la plateforme PLANETE CSCA RH) »*
>
> ***Laurent Devorsine***

Une bonne formation ne suffit pas à faire face à un problème survenu chez un prestataire.

Par exemple, lorsqu'un éditeur de logiciel se fait hacker, l'activité de l'entreprise cliente peut être paralysée. C'est pourquoi, en tant que syndicat, PLANETE CSCA devrait engager un dialogue avec les éditeurs de logiciels de la profession afin d'obtenir des garanties en matière de prise en compte du risque cyber.

[48] *Audition Laurent Devorsine, 25 novembre 2022*

TÉMOIGNAGE[49] DE LAURENT DEVORSINE, CABINET DEVORSINE, VICTIME D'UNE TENTATIVE DE PHISHING

Notre cabinet travaille sur plusieurs pôles et notamment un, celui de l'immobilier, qui génère de nombreux échanges, souvent en urgence, avec les syndicats d'immeuble.
Aussi, malgré un niveau d'information important sur les risques cyber des équipes du cabinet, une assistante a ouvert un lien dans un mail nous demandant un devis, et provoquant immédiatement l'ouverture d'un pop-up semblable à Outlook, l'invitant à rentrer ses codes d'accès.

Dans le même temps, un administrateur système a été victime de la même tentative. Nous avons contacté notre client qui nous indiquait s'être fait pirater.
Notre prestataire est intervenu immédiatement, et tout a pu être réglé en 20 minutes.
Cet exemple démontre que malgré une certaine maturité sur ces sujets, la qualité des mails pirates atteint un tel niveau, que la prévention de suffit plus, mais qu'il est nécessaire de disposer d'une protection renforcée.

Même quelqu'un de très informé peut se faire piéger. Ce qui nous a notamment sauvé, c'est la double authentification nécessaire à l'accès de nos systèmes. Si cela nous était arrivé il y a ne serait-ce que 2 ans, cela aurait pu être dramatique.
C'est pourquoi, il est impératif d'être informé, formé, protégé (notamment par la double authentification) et de disposer d'une intervention rapide d'un spécialiste.
Cet évènement nous a fortement touché et à la suite de notre réflexion ces derniers mois, nous développons un système de gestion des risques pour nos clients, en complément de l'accompagnement assurantiel.

[49] *Témoignage du 21 juin 2023*

Ce risque identifié représente un réel défi pour la profession car il fait apparaître de nouveaux besoins auxquels les assureurs et réassureurs doivent répondre. Ainsi, la qualité des données représente le premier risque pour lequel de nouveaux besoins peuvent émerger et qui peut appeler des solutions assurantielles. Le dynamisme de ces risques technologiques alimente les attentes des populations auprès de la profession en termes de demandes de protections.

Des concertations entre professionnels de l'assurance ont également été conduites afin de définir les actions communes de mise en conformité de l'ensemble du secteur. Il est dans l'intérêt de tous les acteurs de converger vers plus de processus partagés dans les modes de fonctionnement, les formats de données et les outils. Cette réflexion[50], au centre de nombreux échanges d'informations entre assureurs et courtiers, a donné naissance à une initiative concrète financée à 100 % par les assureurs : proposer une plateforme d'échange sur la conformité, unique, gratuite et sécurisée. Les courtiers peuvent ainsi communiquer une seule déclaration de conformité à l'ensemble de leurs partenaires sur les points essentiels attendus par la réglementation.

Les intermédiaires en assurance entretiennent une relation de confiance avec leurs clients. Si ceux-ci apprennent que leurs données ont disparu par manque de sécurisation du cabinet de courtage, la relation de confiance peut se rompre.

En effet, les habitudes prises dans d'autres secteurs ont modifié les attentes, voire les besoins des clients (entreprises comme particuliers) par rapport à leur assureur :

- Un accès à une assistance réactive et immédiate,
- Une personnalisation de la relation ;
- Une digitalisation de l'espace-client, où les canaux à distance (application mobile et site internet) sont devenus les premiers réflexes.
- Un point d'entrée unique et une identification simple quel que soit le produit détenu
- Un parcours client favorisant l'autonomie et allégeant le temps de gestion administrative

Avec cette numérisation, les clients sont donc plus exigeants quant à leurs données.

[50] *Orchestrée par EDICourtage*

Mais jusqu'à récemment, les entreprises protégeaient essentiellement leur système d'information au travers d'une sécurité de type périmétrique. Une barrière est dressée autour de l'infrastructure, afin d'empêcher les pirates de pénétrer le système. Or aujourd'hui, ce modèle ne tient plus, car la notion de périmètre n'existe plus (cloud, connexion extérieure …).

C'est ainsi que cette notion de cyber sécurité s'adapte à ces changements en identifiant un nouveau périmètre : l'utilisateur. Ce dernier est reconnu au travers d'un processus d'authentification, jusqu'alors basé sur la saisie d'un identifiant et d'un mot de passe. Ce procédé n'est plus sûr, et on a vu apparaitre l'authentification multi facteur (MFA).
Il s'agit d'une méthode d'authentification dans laquelle l'utilisateur fournit au minimum deux facteurs de vérification pour accéder à une ressource.
Comme toute mesure de sécurité, l'authentification multi facteur n'est pas infaillible. Cependant, elle réduit significativement le risque de fuite ou de réutilisation de données personnelles par rapport à une authentification simple. La CNIL recommande donc d'activer l'authentification multi facteur chaque fois qu'un service le propose.

Depuis fin 2019[51] , les banques et les prestataires de services de paiement doivent mettre en œuvre une authentification multifacteur pour la plupart des paiements à distance, l'accès au compte ainsi que les opérations sensibles (ajout de bénéficiaire de virements, commande de chéquier, changement d'adresse, etc.).

L'une des pistes pour simplifier l'authentification des utilisateurs, dans un environnement sécurisé, est l'identité numérique[52].

La création d'une identité numérique relève de solutions déjà offertes par différents tiers de confiance. Elle repose sur la combinaison unique d'un identifiant, d'une application mobile et d'un code secret. Les activités des assurances sont de grosses consommatrices de données certifiées. Et le gain peut être substantiel pour une entreprise qui adopterait des parcours clients intégrant l'identité numérique. Par exemple, un établissement bancaire estime ainsi à 20 % le temps gagné lors de l'ouverture d'un compte.

[51] *Directive DSP2*
[52] *Audition Laurent Perret, 1er mars 2023*

La Commission Européenne a lancé en 2019 le processus de révision de son règlement de 2014. Elle cherche « à améliorer son efficacité, étendre ses avantages au secteur privé, à promouvoir des identités numériques fiables pour tous les Européens, et à créer une identité numérique européenne sûre et interopérable qui donne le contrôle aux citoyens ».

Assureur de spécialités, le groupe BEAZLEY[53] est un groupe international d'assurances dont le métier est d'apporter une expertise et une valeur ajoutée à des secteurs de niche. Beazley est l'un des leaders mondiaux du risque cyber depuis dix ans et a géré un grand nombre de sinistres. Aujourd'hui, Beazley partage ses expériences avec les courtiers et les clients afin de les accompagner.

Dans ce contexte, Beazley s'est renforcé dans le cyber, et propose un ensemble de services et d'expertises stratégiques, afin d'améliorer la sécurité des entreprises, en mettant leur expertise des grands comptes au service des TPE et PME.

Depuis 30 ans, toutes les entreprises ont dû se digitaliser, mais n'ont pas immédiatement réalisée les conséquences, et notamment l'arrivée d'un nouveau risque, le risque cyber.

Luc Vignancour
Responsable Souscription Cyber chez Beazley

[53] *Audition du 15 juin 2023, Michèle Horner, Head of European Broker Relations Beazley France*

La plupart des attaques qu'on observe aujourd'hui sont opportunistes. Les sociétés maîtrisent peu leur surface d'exposition : les pirates n'ont qu'à rechercher les portes ouvertes. La solution ne se résume pas à empiler des produits de sécurité. Une bonne approche comporte une analyse des risques suivie par une identification des contrôles pour couvrir ces risques. Les contrôles peuvent se baser sur des changements de pratiques et de comportement, ou sur des produits de sécurité : une fois qu'un bon produit est sélectionné, il faut bien le configurer et l'exploiter pour le rendre efficace et efficient

Jad Nehmé
Cyber Services et Client Expérience Manager - chez Beazley.

Il faut aujourd'hui démystifier le risque cyber, se familiariser avec les menaces et ces risques. Dès lors que nous sommes connectés en réseau, sur le Web ou en lien avec les réseaux sociaux nous exposons notre entreprise à une attaque cyber. L'assurance cyber est avant tout un complément à la gestion du risque de l'entreprise, aussi bien avec sa partie service qu'avec sa partie assurantielle.

Aujourd'hui, la plupart des TPE-PME n'ont pas le niveau de sécurité informatique nécessaire contre les cyber-attaques.
Voici les quatre obligations minimums pour qu'une entreprise puisse s'assurer en cyber :

- Déployer des outils de prévention et de détection d'intrusion ;
- Faire des sauvegardes et le protéger contre les attaques ;
- Former leurs collaborateurs à la cybersécurité et les sensibiliser aux menaces potentielles ;
- Maintenir ses systèmes informatiques (équipements et logiciels) à jour.

En ce sens, en préambule à la contractualisation d'un produit, Beazley a établi un questionnaire simple parmi les plus courts du marché. Pour vendre du cyber, les courtiers ont besoin d'être accompagnés et attendent des exemples pour comprendre et expliquer la démarche à leurs assurés. Beazley a une expérience de dix ans de sinistres cybers et nous partageons cette expérience avec nos courtiers et nos clients.

Michèle Horner
Head of European Broker Relations Beazley France

Depuis le lancement des produits cyber en 2009, Beazley a aidé ses clients à gérer plus de 4 500 attaques informatiques.
C'est l'un des rares assureurs à disposer d'une équipe interne exclusivement dédiée à l'assistance de ses assurés lors d'une attaque, la solution Beazley est une solution leader de cyber-assurance, enrichie de prestations de gestion de crise à la suite d'une violation de données. Le service BBR de Beazley coordonne les services juridiques ainsi que les services d'expertise après sinistre, de notification et de suivi de la notoriété dont les clients ont besoin afin de respecter l'ensemble des exigences légales et de préserver la confiance de leur clientèle.

Au-delà de la coordination de la réponse face aux violations de données, les services BBR mettent à jour et développent la suite de services de gestion des risques de Beazley, spécialement conçus pour minimiser les risques de violations de données.

Plus largement pour ***Michael Monerau*, PDG de la société QONTROL**, le développement de l'assurance cyber PME vient dans un second temps, après que la maturité cyber soit correcte. Pour une PME, souscrire une assurance cyber a du sens après qu'elle ait atteint un niveau minimum de compréhension, de sensibilisation et de compétences. Le développement de l'assurance est un outil pour stabiliser le tissu économique en transférant le risque résiduel.

Il est nécessaire que ce risque résiduel soit faible. Le développement de l'assurance ne doit pas être un frein à l'équipement de l'entreprise (faux sentiment de sécurité par transfert du risque). ●

ENQUÊTE

La réflexion sur l'importance de la cybersécurité dans le secteur de l'intermédiation en assurances doit partir d'une analyse de la perception du boom digital et numérique qui a métamorphosé le monde et donc le secteur.

Alors que beaucoup d'entreprises françaises restent dans le déni face à la cybermenace, les intermédiaires en assurances seront-ils acteurs de la cybersécurité ou victimes de cette innovation ? Où en sont les courtiers dans leur perception du risque ?

Pour répondre à ces questions, PLANETE CSCA a mené une enquête auprès de l'ensemble de ses adhérents. Cet échantillon est distribué sur toute la France et représente la diversité du secteur entre acteurs locaux, régionaux ou nationaux[54].

Parmi les cabinets ayant répondu à l'enquête :

- 42 % emploient entre 1 à 5 collaborateurs
- 26 % n'emploient aucun collaborateur
- 10 % emploient entre 6 et 10 collaborateurs

L'échantillon représente majoritairement le tissu économique des cabinets de proximité, qui constituent, comme vu précédemment, des cibles faciles à atteindre. Seulement 22 % des cabinets ayant répondu emploient plus de 11 collaborateurs. ●

LA VISION GLOBALE DU RISQUE CYBER

86 % pensent que les cabinets de courtage sont particulièrement concernés par ce nouveau risque

Pourtant seulement :

- **49 %** affirment connaitre les différentes menaces cyber.
- **44 %** affirment connaitre les solutions d'assurance cyber et les acteurs de ce marché.

[54] *241 adhérents ont répondu à l'enquête*
[55] *Du numérique à l'intelligence artificielle, Intermédius, 2018*

L'enquête révèle que les courtiers en assurances sont largement conscients de l'impact de ce nouveau risque sur leur activité. Une précédente étude avait montré que les courtiers se perçoivent à une grande majorité comme travaillant au sein de cabinets où les avancées technologiques sont de plus en plus présentes[55]. De ces avancées doivent découler une forte sécurité numérique puisqu'une cyber attaque peut provoquer une fuite de données sensibles et confidentielles ce qui entrainerait une atteinte à la réputation des cabinets mais aussi un préjudice en paralysant l'activité commerciale.

Pour faire face au boom du risque cyber, il est nécessaire que les cabinets se donnent les moyens en termes d'investissements, de développement d'outils, de recrutement et de formation des hommes. ●

LA PRISE EN COMPTE DU RISQUE CYBER AU SEIN DES CABINETS

- 53 % des cabinets disent avoir été victime d'une attaque informatique, principalement sous forme de rançongiciels
- 74 % des cabinets changent les mots de passe des ordinateurs de bureau 1 fois tous les 6 mois
- 94 % mettent régulièrement à jour les logiciels, automatiquement, dès que cela apparait comme nécessaire
- 92 % des ordinateurs professionnels sont équipés d'une protection (antivirus, firewall, solution antispam, etc.) et disposent d'un outil de sauvegarde (support externe, cloud, serveur de stockage interne, etc. ..)
- 53 % protègent leurs données sur le portable (désactivation des fonctions wi-fi et bluetooth, sauvegarde de données, vérification de mots de passe pré-enregistrés, etc.)
- 72 % déclarent séparer les usages personnels des usages professionnels
- 51 % des cabinets disent avoir investi dans la cyber sécurité :
  - › Contrat d'assurance dédié (73 %)
  - › Opération de sensibilisation des salariés (68 %)
  - › Renforcement des équipes en charge de la protection des systèmes d'information (27 %)
  - › Acquisition de nouveaux outils informatiques (68 %)

- L'autre moitié n'investit pas dans la cyber sécurité :
  - › par manque de temps (54 %)
  - › par manque de budget (41 %)
  - › par manque de prise de risque (28 %)
  - › par manque de compétence (23 %)
- 42 % des cabinets tentent de sensibiliser leurs collaborateurs au risque cyber tous les 6 mois, dans la majorité des cas, cette sensibilisation est assurée par le dirigeant.

La sécurisation informatique a longtemps été négligée dans les entreprises. La mise en application du RGPD en 2018 a accéléré la prise de conscience des risques liés à la sécurité informatique par les entreprises et en premier lieu l'exigence de protection de données personnelles.

Les intermédiaires en assurances s'assurent de maintenir leur système d'information parfaitement à jour pour garantir le meilleur niveau de sécurité possible. Les cabinets tentent d'adopter une gestion rigoureuse et limitée des droits d'accès aux différents outils et aux données de l'entreprise, réduite au strict nécessaire particulièrement lorsqu'il s'agit des dossiers client du cabinet.

Au-delà de la qualité et du niveau de sécurité apportés par les outils techniques, l'entreprise se doit d'inculquer une véritable culture de la sécurité à tous ses collaborateurs afin de les sensibiliser à la cybersécurité au bureau mais également en télétravail. Certains cabinets considèrent qu'en intégrant ce risque dans la stratégie, la gouvernance d'entreprise pourra mettre en œuvre une organisation à même de détecter une attaque le plus rapidement possible afin de limiter l'impact financier et permettre de reprendre l'activité rapidement. C'est le cas des grands cabinets de courtage qui sont équipés de direction cyber, constamment en formation face à un risque évoluant quotidiennement[56]. ●

[56] *Audition Lari Lehtonen, 8 novembre 2022*

LA PRISE EN COMPTE DU RISQUE CYBER DANS L'ACTIVITÉ DE CONSEIL AUPRÈS DES CLIENTS

- 70 % rencontrent des difficultés pour trouver des solutions cyber

- 63 % des cabinets ne proposent pas la prévention au risque cyber à leurs clients notamment à cause de leur manque de compétence sur ce sujet

Les intermédiaires en assurance affirment mettre en œuvre les outils nécessaires au sein de leurs cabinets pour anticiper les cyber attaques mais l'effort apparait insuffisant à l'échelle des cabinets de proximité lorsqu'il s'agit de présenter l'enjeu aux clients.

L'enquête nous révèle que le risque cyber est mal pris en compte dans l'activité de conseil auprès des clients. Si cette démarche d'analyse du risque n'est pas correctement effectuée, les courtiers en assurance peuvent rencontrer des problèmes pour conseiller correctement leurs clients[57]. C'est après l'analyse du risque, qui consiste à bien regarder si la garantie d'assurance peut couvrir le risque de l'entreprise, que démarre la seconde étape. Celle-ci va permettre de s'assurer que l'entreprise a atteint un niveau de maturité cyber suffisant (c'est-à-dire confirmer l'assurabilité de l'entreprise). C'est seulement dans ce cas que l'on lance une démarche d'assurance cyber.

La cybersécurité est aussi un enjeu d'image. Partenaire de confiance des entreprises et des consommateurs, les courtiers en assurances doivent se démarquer et apporter une plus-value renforcée à leurs clients. Ils doivent monter en compétence afin de pouvoir appréhender le risque et éduquer, à leur tour, les clients. Alors que de nombreuses attaques perturbent la continuité de service, le courtier doit démontrer sa maîtrise de la question afin de conserver la confiance de son client.

Si l'assurance est essentielle pour des courtiers qui cherchent à se prémunir du risque cyber, la formation occupe également une place importante dans le processus de protection d'un cabinet de courtage.
Afin que les courtiers puissent, dans un second temps, conseiller des assurances cyber à leurs clients, ils doivent maîtriser ce risque. Dans une récente enquête, France Assureurs[58] constate que la majorité des intermédiaires en assurance n'est pas à l'aise avec cette question.
Les courtiers en assurance doivent rassurer leurs clients. Ils doivent avoir un discours pédagogique et non anxiogène.
Les intermédiaires en assurance doivent être mobilisés autour de cette thématique.

[57] *Audition Lari Lehtonen, 8 novembre 2022*
[58] *Audition Christophe Delcamp, France Assureurs, 22 novembre 2022*

À titre d'exemple, France Assureurs et agéa organisent régulièrement des ateliers de formation avec la gendarmerie pour les agents généraux. 800 agents généraux ont été formés depuis le lancement de cette opération.
Le lien de cause à effet n'est pas établi mais force est de constater que les primes d'assurance cyber sont en fortes augmentation : x2,5 sur la période 2018 - 2021.

L'approche des TPE-PME et celle des grandes entreprises sont complètement différentes.
Les « grands comptes » apparaissent comme plus « matures » face à ce nouveau risque et cela génère des exigences plus élevées vis-à-vis des assureurs, qui doivent revoir leur offre en conséquence.
À contrario, les couvertures assurantielles sont aujourd'hui adaptées pour les TPE / PME, mais ce sont les entreprises qui ne sont pas prêtes.

De manière générale depuis le Covid, il devrait y avoir une prise de conscience du coût du risque. Les assureurs et leurs clients devraient se rendre compte que le risque cyber devait apparaître dans les garanties.
Même s'il se développe très rapidement, le marché n'a pas encore la masse critique pour absorber les grands chocs qui pourraient survenir. La mutualisation est encore insuffisante, le développement du marché des TPE / PME est donc nécessaire. ●

LE MARCHÉ DE L'ASSURANCE RISQUE CYBER

Spécialiste du Risk management, l'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) a publié, en 2021, sa 1re étude Lucy (LUmière sur la CYberassurance) posant la question de l'assurabilité du risque cyber : après une année 2020 fortement déficitaire, les assureurs ont alors semblé vouloir se retirer du marché.

La 3e édition de l'étude LUCY[59], publiée en mai 2023, s'appuie sur un historique de quatre ans de données objectives, globales, représentatives et robustes.
Produites par les meilleurs observateurs du risque d'entreprises, 10 courtiers et PLANETE CSCA ont répondu au questionnaire conçu de façon collaborative par l'AMRAE.
Cette étude permet de comprendre le marché mais également d'anticiper ses évolutions.

Les conclusions de l'étude LUCY révèlent que :

- Après avoir fortement baissé en 2020 et 2021, le marché de l'assurance cyber est revenu en territoire positif. Ce risque, qui semblait inassurable il y a peu, a de nouveau attiré les assureurs en 2022.

- Après trois ans d'augmentation, les taux de prime ont semblé marquer le pas fin 2022, incitant les entreprises à s'assurer à la hauteur de leur exposition.

- Les PME suivent la même courbe d'apprentissage que les grandes entreprises et les ETI. L'assurance cyber pénètre progressivement toutes les strates de notre tissu économique.

- Le marché de l'assurance cyber semble avoir trouvé une forme d'équilibre. La hausse du taux de couverture des entreprises et la baisse de la sinistralité sont des signaux positifs, de nature à accélérer la croissance du marché.

- Mais cet équilibre est encore fragile : le volume total de primes encaissées en France au titre de la garantie cyber est équivalent au coût d'un très gros sinistre cyber. Une attaque de grande ampleur suffirait à remettre cet équilibre en question.

- La guerre en Ukraine n'a pas eu pour effet d'augmenter le nombre d'attaques cyber en France. Mais rien ne dit que ce sera toujours le cas dans les mois ou les années à venir.

[59] *Intégralité de l'étude https://www.amrae.fr*

Autre élément d'incertitude sur la sinistralité : l'intelligence artificielle pourrait accroître la fréquence et l'intensité des attaques cyber.

Les assureurs restent prudents à l'égard d'un risque encore volatil. Signe de cette prudence, le Lloyd's de Londres a décidé de modifier la couverture des actes de cyberguerre.

Ces nouvelles conditions de souscription pourraient réduire l'appétence des entreprises à l'égard de l'assurance cyber.

Pour améliorer l'attractivité des couvertures cyber, les assureurs ont intérêt à simplifier les process de souscription et à les adapter à la taille des entreprises. ●

RECOMMANDATIONS

SENSIBILISATION & PRÉVENTION

- Mettre en place des ateliers de sensibilisation et de formation en ligne dans le cadre de l'offre de formation de PLANETE CSCA RH
- Étudier la faisabilité de la mise en place d'une certification interbranches en cybersécurité
- Communiquer sur les protocoles
- Cybermalveillance et les prestataires labélisés ExpertCyber dans les territoires (campagne commune ou partenariat avec Cybermalveillance)
- Promouvoir les bonnes pratiques des adhérents
- Intégrer les réseaux d'accompagnement des TPE-PME (cybermalveillance, cybercampus...) dans le cadre de la stratégie d'intégration territoriale de PLANETE CSCA

CULTURE DE LA CYBERRÉSILIENCE

- Expliquer la démarche de cyberrésilience
- Instaurer une culture de la cyberrésilience grâce à une interrogation régulière des adhérents permettant d'identifier les alertes et de diffuser les bonnes pratiques
- Engager un dialogue exigeant avec les éditeurs de logiciels de la profession afin d'obtenir des garanties en matière de prise en compte du risque cyber

MISE EN PLACE D'OUTILS

- Contribuer à la création d'une identité numérique impulsé par PLANETE CSCA
- Construire un partenariat avec un acteur spécialiste du cyber-risque afin d'organiser des campagnes-tests de phishing et, à terme, de commercialiser un produit de prévention et de couverture du risque
- Développer un outil commun à la profession, décliné à chaque cabinet
- Construire et diffuser pour les adhérents, mais aussi auprès des clients, un outil de diagnostic des risques

DÉVELOPPER L'ASSURANTIEL

- Accompagner les courtiers dans cette démarche de proposition d'assurance cyber
- Donner accès à un ensemble complet de solutions conçues pour une protection à 360° contre le risque cyber.

L'étude réalisée auprès des adhérents de PLANETE CSCA nous permet d'affirmer que les courtiers en assurances ont une prise de conscience face aux enjeux cyber. Pourtant les défis sont encore nombreux. À travers ces recommandations, l'institut Intermédius imagine comment le syndicat pourrait accompagner les cabinets de courtage face au risque cyber et positionner la profession comme un acteur crédible de la maîtrise du risque cyber.

À travers leurs travaux de prospection, l'institut Intermédius et PLANETE CSCA manifestent leur souhait de faire évoluer la profession et de l'accompagner dans son évolution. Ces travaux ont vocation à s'inscrire dans la durée. C'est pourquoi, ils s'engagent à assurer le suivi des recommandations et leur mise en œuvre.

Retrouvez tous les livres blancs d'INTERMEDIUS sur notre page dédiée sur www.planetecsca.fr !

Conception et réalisation
par INTERMEDIUS et PLANETE CSCA

LE TRI + FACILE BROCHURES BAC DE TRI

PLANETE CSCA

LE SYNDICAT DES COURTIERS D'ASSURANCES

NOUS CONTACTER

10 rue Auber
75009 PARIS

01 48 74 19 12
www.planetecsca.fr

CGPA

vivre votre profession avec assurance

NOUVEAU

SERVICES CYBER OFFERTS

NOUVEAU

VOTRE RC PRO VOUS AIDE AUSSI À PRÉVENIR LES RISQUES CYBER

Les risques liés aux technologies numériques ne cessent d'augmenter et peuvent affecter votre activité.
C'est pourquoi CGPA, leader de la RC Pro des intermédiaires d'assurance, a décidé d'offrir à ses clients un programme de services en ligne leur permettant de mieux identifier les menaces cyber et d'améliorer leurs réflexes pour s'en prémunir.

QUIZ ET REPÈRES PRATIQUES
DÉTECTION DE FUITE D'ADRESSES MAILS
PHISHING GAME

www.cgpa.fr

REJOIGNEZ -NOUS !

ET DÉCOUVREZ TOUS LES SERVICES POUR LES ADHÉRENTS

PLANETE CSCA

LE SYNDICAT DES COURTIERS D'ASSURANCES