Dauphine | PSL
EXECUTIVE EDUCATION

Executive MBA Centre des Hautes Etudes d'Assurances

LES PME FRANÇAISES ET LA PROTECTION CONTRE LE RISQUE CYBER

Antoine Bergonzat - Laurent Decelle - Amandine Lezy - Christophe Valero

Promotion 2022 / 2023

Octobre 2023

Remerciements

Nous tenons avant tout à remercier sincèrement les deux co-directeurs du CHEA, Frédéric Gonand et Olivier Muraire, ainsi qu'Isabelle Pasquet pour leur accompagnement tout au long de la formation et de la rédaction de ce mémoire.

Nous remercions également les personnes qui ont bien voulu nous accorder de leur temps afin de partager leur expertise dans le cadre des travaux relatifs à ce mémoire :

- Christophe ARREBOLLE, Président et Alexis NARDONE, Directeur général, INQUEST, société spécialisée en expertise de sinistres cyber ;
- Marc BOTHOREL, Gérant de PORTER CONSULTING EUROPE, Consultant en cybersécurité pour HP France et Référent national cybersécurité pour la CPME (Confédération des Petites et Moyennes Entreprises) ;
- Arnaud CHNEIWEISS, Médiateur de l'assurance ;
- Stéphanie CONTE et Franck LOURDELET, Responsables Partenariats, HISCOX France
- Charlotte COUALLIER, Co-fondatrice et CEO, DATTAK ;
- Christophe DELCAMP, Directeur des assurances de dommages et de responsabilité, FRANCE ASSUREURS ;
- Valentin GERVIT, Secrétaire général, MEDEF 79 ;
- Sébastien HEON, *Deputy Chief Underwriting Officer – Cyber Solutions*, SCOR ;
- Charlotte JEPHOS, *Claims Manager*, Beazley ;
- Bastien MARCHIVE, Député de la 1ère circonscription des Deux-Sèvres, membre de la Commission des affaires économiques à l'Assemblée nationale ;
- Hervé MASUREL, Directeur commercial adjoint Entreprises et Professionnels, PACIFICA ;
- Florian PRISSÉ, Agent général MMA.

Introduction

Aujourd'hui, le monde entier subit de profonds changements sous l'effet d'une société toujours plus numérique. La digitalisation et l'avènement d'un cinquième pouvoir[1], celui de la donnée, sont porteurs de réelles opportunités et de nouveaux marchés pour notre économie. Les techniques digitales de communication facilitent l'information, la concurrence, la baisse des prix, l'innovation dans la plupart des domaines, au profit des consommateurs ; l'intelligence artificielle, même si elle doit être régulée, est notamment pourvoyeuse de progrès dont notre société continuera à profiter pour longtemps.

Cependant, **la numérisation et les interconnexions de toutes natures favorisent également les possibilités d'attaques informatiques**[2]. Tout un monde parallèle y voit l'opportunité de s'enrichir ou de terroriser des Etats comme des particuliers, des administrations ou des entreprises, en se saisissant des failles informatiques ; la cybercriminalité pouvant être définie en tant qu'acte malveillant visant à altérer les systèmes d'information[3]. Comme le résume Agathe Lepage, professeur à l'Université Panthéon-Assas[4] : "Pieds et mains liés au numérique, les sociétés contemporaines y puisent ce qui les rend aussi performantes que fragiles, dans un témoignage édifiant de l'ambivalence du numérique".

Or **les petites et moyennes entreprises françaises sont particulièrement exposées** : la numérisation leur offre de nombreuses opportunités (conquête de nouveaux marchés, amélioration de la relation client…) mais les fragilise en parallèle en mettant leurs actifs et leurs données à la portée des cybercriminels. Leur niveau de sécurité informatique est hétérogène, **le taux de couverture des PME en assurance cyber est proche de zéro**, alors que ce risque est désormais considéré comme la première menace pour les entreprises[5]. Ainsi, **une cyber attaque sur deux[6] en France vise aujourd'hui les PME**.

[1] Michel Serres, « Petite Poucette», Le Pommier, mars 2012 : « la donnée un nouveau pouvoir indépendant des 4 autres, législatif, exécutif, judiciaire et médiatique »
[2] S. Héon et D. Parsoire, "La Couverture du cyber risque", The Geneva Papers on Risk and Insurance, février 2017
[3] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[4] Le Club des juristes, "Le Droit pénal à l'épreuve des cyberattaques", préface, avril 2021
[5] CESE, "Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques", avril 2022
[6] ANOZR WAY, "Baromètre du *ransomware*, 5ème édition", janvier 2023 - étude portant sur plus de 3 000 attaques

En 2018, le secrétaire d'État au numérique[7] s'exprimait déjà sur la nécessité d'améliorer la protection des PME françaises : « si demain, 25 000 PME tombent le même jour, c'est l'État français qui sera menacé », exprimait avec gravité Mounir Mahjoubi.

Les PME françaises vivent donc un réel défi de cybersécurité et le rôle des assureurs sera crucial pour accompagner ce mouvement. Les conséquences systémiques du Covid-19, et le contexte économique actuel difficile nous motivent à faire **des propositions concrètes et applicables à court et moyen terme.**

Dans la première partie de ce mémoire, après avoir défini les principaux concepts, nous décrirons et analyserons la situation actuelle des PME françaises qui sont fortement exposées au risque cyber. Quelles en sont les raisons ? Quels sont les principaux freins à une meilleure protection ?

Dans la seconde partie, nous proposerons nos recommandations, tant sur la prise de conscience, l'accompagnement, que la prévention des PME françaises avant de motiver des actions qui doivent permettre de débloquer la situation du marché français de l'assurance cyber. Pour ce faire, nous utiliserons tous les appuis pertinents, allant du concours de l'Etat et des pouvoirs publics, des organisations professionnelles, à celui des assureurs.

Nos travaux ont été éclairés par des échanges réguliers avec des sachants du domaine cyber et de l'écosystème des PME, avec lesquels nous avons pu partager nos constats, analyses et leviers d'amélioration, durant cette année 2023.

[7] Mounir Mahjoubi, Forum International de la Cybersécurité, Lille 2018, cité dans le rapport de l'Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018

Sommaire

I. L'analyse de la situation actuelle : des PME françaises peu protégées contre le risque cyber

A. Les PME et le risque cyber en France

Dans un premier temps, nous nous attacherons à définir les principaux concepts et à décrire le marché spécifique des PME et leur exposition face au risque cyber.

1. Etat des lieux de la menace cyber pour les PME françaises

Il convient tout d'abord de rappeler **la définition des PME et leurs poids au sein de l'économie française**. Les PME sont définies dans la loi de Modernisation de l'Économie[8].

Elles englobent les **microentreprises**, celles dont l'effectif est inférieur à 10 personnes et dont le chiffre d'affaires ou le bilan annuel n'excède pas 2 M€. Celles-ci sont pour majorité des entreprises individuelles, c'est-à-dire sans salarié.

Viennent ensuite les **petites entreprises**, sociétés dont l'effectif se situe entre 10 et 49 salariés et dont le chiffre d'affaires et le bilan ne dépassent pas 10 M€ par an ; et, enfin, les **moyennes entreprises,** avec des effectifs compris entre 50 et 250 salariés et dont le chiffre d'affaires et le bilan sont respectivement inférieurs à 50 M€ et 43 M€.

La France compte 4,2M de petites et moyennes entreprises marchandes non agricoles et non financières[9]. Parmi elles, les 4,08M de microentreprises constituent l'immense majorité des entreprises françaises. Au global, les PME représentent 46% des emplois français, soit plus de 6M[10]. Elles réalisent 1 415 Mds€ de chiffre d'affaires annuel (37 % du total français), 43% de la valeur ajoutée du tissu productif français et 15% des exportations.

En termes d'activité, (en excluant les micro-entreprises), les services représentent 31% des PME, le commerce 28%, l'industrie 18%, la construction 17% et les transports 6%.

[8] Décret n° 2008-1354 (article 51) du 18 décembre 2008
[9] Insee, "Les Entreprises en France - édition 2022", décembre 2022
[10] En équivalent taux plein

Les PME sont ainsi la "colonne vertébrale" de l'économie française, par leur vitalité, leur nombre ou encore leur capacité à mailler le territoire, et, par conséquent, à faire rayonner une activité économique dans l'ensemble de l'hexagone.

Ces PME n'échappent pas à la **rapide digitalisation** de l'économie française, qui s'est accélérée avec la pandémie du Covid-19 et qui, à son tour, rend le **risque cyber plus prégnant**. Deux statistiques illustrent ce phénomène :

- 68% des entreprises françaises disposent d'un site internet en 2022 contre 37% en 2020[11] ;
- Lors du premier confinement lié à la pandémie au printemps 2020, le recours massif au télétravail s'est accompagné d'une croissance de 667% des attaques par *phishing* entre le 1er et le 23 mars 2020[12].

Le **risque cyber** peut être défini comme un **risque opérationnel portant sur la confidentialité, l'intégrité ou la disponibilité des données et des informations**[13]. Il recouvre aussi bien des incidents non intentionnels issus d'erreurs humaines ou d'accidents que des actes malveillants ; ces derniers représentent aujourd'hui la vaste majorité du cyber risque[14].

La **cybercriminalité** a connu un **développement extrêmement rapide** ces dernières années. Son coût mondial est estimé 8 000 Mds$[15] en 2023. Au-delà de la numérisation de l'économie, trois facteurs expliquent cet essor :

- **La difficulté de la répression** (faible capacité à identifier et à localiser les criminels) ;
- Le développement depuis quelques années d'une offre de **"*Ransomware as a Service*"** avec la capacité d'avoir accès, pour une somme modique, à un "kit" rassemblant l'ensemble des produits et services dont ont besoin les criminels[16] : aujourd'hui ces offres sont disponibles à partir de 40 $ par mois[17]. Elles continuent de se professionnaliser et de se sophistiquer, avec notamment un recours accru à l'IA[18]. Ainsi, **la cybercriminalité est devenue "*low cost*"**[19] ;

[11] Institut Montaigne, "Cybersécurité : passons à l'échelle", juin 2023
[12] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[13] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[14] A titre illustratif, les attaques externes représentent plus de 80% de la valeur des 3 000 sinistres cyber d'Allianz sur les cinq dernières années. Allianz, "*Cyber: The Changing Threat Landscape*", octobre 2022
[15] Cyber Security Ventures, "*2022 Official Cybercrime Report*", décembre 2022
[16] ENISA, "*Threat Landscape 2023*", octobre 2023
[17] Allianz, "*Cyber security trends 2023*", octobre 2023
[18] PwC, "*Cyber Threats 2022: A Year in Retrospect*", mai 2023
[19] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021

- L'apparition des **crypto monnaies** qui facilite le blanchiment du paiement des rançons[20].

Aujourd'hui, les **principales catégories d'attaques ou d'intrusions cyber** peuvent être décrites comme suit[21] :

- L'**hameçonnage** (ou *phishing*) est une technique frauduleuse destinée à leurrer l'utilisateur pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un *mail*, d'un SMS ou d'un appel téléphonique d'une banque… L'hameçonnage ne cesse de progresser et a représenté 37 % des recherches d'assistance sur cybermalveillance.gouv.fr en 2022[22] ;

- Le programme malveillant (ou *malware*), dont le **rançongiciel** (ou r*ansomware*) : ce dernier est un logiciel qui pénètre et bloque l'accès à l'ordinateur ou aux fichiers des victimes et qui leur réclame le paiement d'une rançon pour en obtenir à nouveau l'accès. Fréquemment, les pirates chiffrent les fichiers se trouvant sur l'ordinateur de la victime ou sur des serveurs. Ce chiffrement se double désormais dans plus de trois cas sur quatre d'une exfiltration des données[23], ce qui généralise le phénomène de **double extorsion** (pour récupérer les données encryptées et empêcher la fuite des données).

  Ces logiciels malveillants exploitent généralement les failles de sécurité connues et identifiées des applicatifs (près de 25 000 vulnérabilités publiées entre juillet 2022 et juin 2023[24]). Selon Bessé[25], 90% de ces failles peuvent être exploitées avec des "compétences techniques minimales". Parmi l'ensemble des risques de cybersécurité touchant les entreprises, **le ransomware représente la menace la plus régulièrement observée, notamment pour les PME**[26];

- Les **attaques par DDoS** (*Distributed Denial of Service*) visent à rendre des données ou des systèmes inaccessibles, en exploitant une vulnérabilité ou en saturant la bande passante du réseau par exemple ;

- Les attaques visant les **réseaux sociaux** se multiplient également avec le vol des identifiants de connexion et autres données personnelles ;

[20] Institut Montaigne, "Cybersécurité : passons à l'échelle", juin 2023
[21] ENISA, "*Threat Landscape 2023*", octobre 2023 & S. Héon et D. Parsoire, "La Couverture du cyber risque", The Geneva Papers on Risk and Insurance, février 2017
[22] Cybermalveillance.gouv.fr, "Rapport d'activité 2022", mars 2023
[23] Allianz, "*Cyber security trends 2023*", octobre 2023
[24] ENISA, "*Threat Landscape 2023*", octobre 2023
[25] Bessé, en partenariat avec Stelliant, "Risques cyber : analyse de la sinistralité : quels enseignements ?", octobre 2022
[26] ENISA, "*Threat Landscape for Ransomware Attacks*", juillet 2022

- La **fraude au président** consiste pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte, par exemple, d'une dette à régler ;
- La **perturbation d'infrastructures critiques** : il s'agit d'une attaque visant une interruption ou un dysfonctionnement du processus industriel ou commercial sans dommage physique ;
- Les **attaques informatiques donnant lieu à des dommages physiques** pour des équipements connectés à internet. Celles-ci sont moins connues mais peuvent paralyser les entreprises dont la production est fortement robotisée. Ces attaques permettent aux pirates de prendre le contrôle à distance de systèmes de contrôles dans des usines par exemple.

Les cyberattaques ont pour origine une multitude d'acteurs :

- **Des organisations mafieuses** attirées principalement par le gain financier : elles représentent **l'essentiel des acteurs qui visent les PME françaises** ;
- **Des groupes menaçants liés aux États** : mercenaires ou groupes liés aux services de renseignements étatiques, ces groupes d'attaquants s'inscrivent dans des logiques de sabotage, d'espionnage ou de déstabilisation des États ;
- **Des individus isolés** : leurs motivations peuvent être idéologiques ou financières. Ils peuvent être internes à l'organisation ou externes ;
- **Des hacktivistes**[27] : il s'agit de groupes motivés par des ambitions idéologiques et qui agissent dans le but de dégrader l'image de marque ou la réputation des structures ciblées.

Comme le souligne le Général Marc Boget, à la tête de la stratégie digitale et technologique de la Gendarmerie Nationale, les "chiffres de la cybercriminalité explosent"[28]. **Ces attaques visent de plus en plus les PME** :

- Moins bien protégées que les grands groupes, elles constituent des cibles plus faciles à atteindre ;
- Elles peuvent aussi être spécifiquement visées pour atteindre indirectement les systèmes d'information des plus grandes entreprises dont elles sont les prestataires[29].

[27] Mot-valise provenant de la contraction de « hacker » et « activiste »
[28] Les Echos, "Cyberattaques : les PME en première ligne du risque numérique", 11 octobre 2023
[29] Le Club des juristes, "Le Droit pénal à l'épreuve des cyberattaques", avril 2021

Comme le dit Scott Sayce, Global Head of Cyber d'AGCS[30], la cible préférée des criminels est actuellement une entreprise de taille moyenne avec de faibles niveaux de contrôle, de gestion des risques et de cybersécurité. Hervé Masurel de Pacifica[31] constate que les sociétés détenant des données personnelles sensibles sur leurs clients sont souvent visées.

On observe également que les cyberattaques qui visent les PME ne sont pas de même nature que celles qui touchent les grands groupes. Les plus petites structures font face à une "menace non ciblée, diffuse et courante pouvant toucher tout un chacun"[32], notamment des campagnes de *ransomware* qui les visent de façon opportuniste, massive et indifférenciée[33]. Les grandes entreprises sont davantage exposées à une menace plus sophistiquée et personnalisée[34], insiste Charlotte Couallier[35], CEO de Dattak.

Ces développements ont remodelé en profondeur la cartographie des risques perçus par les assureurs. France Assureurs[36] positionne ainsi le risque cyber en tête de son classement des risques 2023 et ce, pour la sixième année consécutive. Allianz[37] tout comme l'assureur Hiscox[38], qui s'est spécialisé dans l'assurance des PME, confirment cette situation critique, exprimant que **la cybermenace est désormais largement considérée comme le risque n°1 pour l'entreprise**.

L**e risque cyber ne dispose pas de statistiques officielles**. Il n'existe pas en effet de base de données de référence sur le nombre d'incidents cyber. Asterès[39] estime à 347 000 le nombre de cyberattaques réussies en France en 2022, dont 330 000 ayant touché des PME, qui sont donc les premières victimes.

A partir des données Hiscox[40], **52% des entreprises françaises ont été victimes d'une attaque cyber « réussie » en 2022** ; des résultats cohérents avec l'enquête du CESIN, qui estime à 45% la part des organisations françaises ayant été victimes d'au moins une cyberattaque en 2022[41]. **La moitié de ces cyber attaques ont visé des PME[42]**.

[30] Allianz, *"Cyber: The Changing Threat Landscape"*, octobre 2022
[31] Hervé Masurel, directeur commercial adjoint Entreprises et Professionnels de Pacifica, entretien du 25 septembre 2023
[32] Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018
[33] PwC, "*Cyber Threats 2022: A Year in Retrospect*", mai 2023
[34] Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018
[35] Charlotte Couallier, CEO de Dattak, entretien du 13 janvier 2023
[36] France Assureurs, "Cartographie prospective 2023 des risques de la profession de l'assurance et de la réassurance", janvier 2023
[37] Allianz Global Corporate and Specialty, "Baromètre des risques 2023", janvier 2023
[38] Hiscox Assurances, "Rapport 2023 sur la gestion des cyberrisques", 7ème édition, octobre 2023
[39] Asterès, "Etude sur les Cyberattaques réussies en France : un coût de 2Mds€ en 2022", juin 2023
[40] Hiscox Assurances, "Rapport 2022 sur la gestion des cyberrisques", 6ème édition, novembre 2022
[41] Opinion Way pour le CESIN, "Baromètre de la cybersécurité des entreprises", 8ème édition, janvier 2023
[42] ANOZR WAY, "Baromètre du *ransomware*, 5ème édition", janvier 2023 - étude portant sur plus de 3 000 attaques

Les **impacts d'une cyberattaque** s'avèrent souvent dramatiques pour les PME. Faute de sécurisation des systèmes informatiques et de couverture assurantielle, les « sinistres » cyber peuvent en effet compromettre la pérennité des entreprises visées :

- Bessé[43] estime qu'une PME victime d'une attaque cyber double son risque de dépôt de bilan ;
- Une étude de Munich Re[44] conclut qu'en cas de cyber incident, 95% des petites sociétés subissent un impact direct et défavorable sur leurs opérations ;
- InCyber[45] précise concrètement les conséquences des violations sur les données de l'entreprise : dans 2,6% des cas, elles remettent en cause l'intégrité de la donnée, dans 5,7% des cas, elles la rendent indisponible et, enfin, dans 91,6% des cas, elles causent une perte de confidentialité de la donnée ;
- Bessé[46] constate que les délais de retour "à la normale" s'établissent en moyenne entre 25 et 30 jours pour les PME, avec une période de forte perturbation comprise entre 10 et 15 jours ;
- La même étude évalue les coûts d'une cyberattaque à 1 M€ pour une PME et à 200 k€ pour une TPE. Un rapport de NetDiligence[47], qui a analysé plus de 9 000 sinistres cyber dans plusieurs pays, présente des montants moins importants : 125 k$ pour les entreprises avec moins de 50 M$ de chiffre d'affaires et 300 k$ pour les entreprises dont le chiffre d'affaires est compris entre 50 M$ et 300 M$.

Nous dressons également dans cette section un **panorama de l'assurance cyber en France**.

L'assurance cyber est depuis fin 2022 une branche autonome de l'assurance. A ce titre, il n'existe pas encore de données officielles sur le marché de l'assurance cyber en France.

Nos analyses du marché se fondent majoritairement sur les **travaux de l'AMRAE** qui publie depuis trois ans une **étude** nommée **LUCY**[48] (LUmière sur la CYberassurance). Bien que cette étude ne soit pas exhaustive (notamment sur le segment des plus petites entreprises), elle offre une bonne vision globale du marché de l'assurance cyber en France et de ses tendances. L'annexe 1 présente une synthèse de la méthodologie et des principaux résultats chiffrés de l'étude.

[43] Bessé, « Crise cyber : quel impact sur les entreprises non cotées ? », novembre 2020
[44] Munich Re *"Global Cyber Risk & Insurance Survey 2022",* août 2022 - Etude menée auprès de 7 000 participants dans 14 pays
[45] InCyber, "Baromètre fuite de données", mai 2023
[46] Bessé, en partenariat avec Stelliant, "Risques cyber : analyse de la sinistralité : quels enseignements ?", octobre 2022 - Etude portant sur l'analyse détaillée de 59 sinistres cyber entre 2019 et 2021 (dont 56% ont touché des TPE/PME)
[47] NetDiligence, "*Cyber Claims Study 2023 Report*", 13ème édition, octobre 2023. Cette étude porte sur plus de 9 000 sinistres cyber aux Etats-Unis, au Canada et au Royaume-Uni entre 2018 et 2022 et s'appuie sur des données fournies par plus de 18 assureurs cyber
[48] AMRAE, "Etude LUCY" (LUmière sur la CYberassurance), 1ère , 2ème et 3ème éditions, mai 2021, juin 2022 et mai 2023

Le marché de l'**assurance cyber** demeure marginal en France. Toutes entreprises confondues, il totalise **313 M€ de chiffre d'affaires** en 2022, selon France Assureurs[49], soit seulement 4% du total des cotisations en assurance de dommages. Sur un marché mondial de l'assurance cyber estimé à 14 Md$[50], la France pèse pour 2%.

Comme mentionné plus haut, l'assurance du risque cyber reste marginale pour les PME : quand 94% des grandes entreprises sont couvertes, **pour les PME ce taux oscille entre 3%** (pour les entreprises dont le chiffre d'affaires annuel est compris entre 10M€ et 50M€) **et 0,2%** (pour les sociétés avec un chiffre d'affaires annuel inférieur à 10M€)[51]. L'étude note néanmoins une progression de 53% en 2022 du nombre de PME assurées par rapport à 2021[52].

Faute de protection et de couverture en assurance suffisante, l'exposition des **PME françaises** au risque cyber, qui sont aujourd'hui les « **oubliées de la cybersécurité** »[53], est considérable.

La France affiche du retard dans ce domaine : l'indice DESI[54] publié par la Commission européenne classe les PME françaises au 12ème rang communautaire pour leur résilience au risque cyber. Il reste donc du chemin à parcourir pour réduire les risques opérationnels et économiques auxquels sont exposées ces entreprises.

Ceci nous amène à **comparer la situation du marché français au niveau international**.

La gravité du risque cyber s'entend à l'échelle mondiale, comme le souligne Allianz dans son baromètre des risques[55] : la plupart des pays étudiés (Canada, Inde, Italie, Japon, Espagne, Suisse, Royaume Uni, …) classent ce risque comme « risque numéro 1 pour les petites et moyennes entreprises ».

La FERMA, en tant qu'association des *risk managers* européens, pose également le risque cyber en 1ère position pour les entreprises depuis 2018[56]. Le niveau de couverture assurantielle sur le plan mondial est estimé pour les PME à 14%, selon Munich Re[57]. Des écarts importants entre pays existent par conséquent, la France concédant un retard significatif.

[49] France Assureurs, étude statistique "L'Assurance de dommages aux biens des professionnels en 2022", juin 2023
[50] IAIS, "*Global Insurance Market Report - Special Topic Edition - Cyber*", avril 2023
[51] AMRAE, "Etude LUCY" (LUmière sur la CYberassurance), 3ème édition, mai 2023
[52] AMRAE, "Etude LUCY" (LUmière sur la CYberassurance), 3ème édition, mai 2023
[53] François Cazal, Professeur adjoint à HEC Paris et Lieutenant-colonel Réserve citoyenne de la gendarmerie, cité dans Les Echos, "Cyberattaques : les PME en première ligne du risque numérique", 11 octobre 2023
[54] Commission Européenne, "*Digital Economy and Society Index 2022*", juillet 2023
[55] Allianz Global Corporate and Specialty, "Baromètre des risques 2023", janvier 2023
[56] FERMA, "*European Risk Manager Survey Report - 2022*", août 2023
[57] Munich Re, *"Cyber insurance : risks and trends 2023"*, avril 2023

Une analyse des marchés européens fait apparaître un constat globalement en ligne, mais avec des disparités notables selon les pays.

Au niveau européen, la situation globale ne diffère pas de celle de la France, avec des PME fortement exposées au risque cyber mais faiblement couvertes par des polices d'assurance. Le sondage en cours de l'EIOPA[58] sur l'accès des PME à la cyber assurance montre que ce thème est d'actualité et dépasse les frontières nationales.

Selon Beazley[59], acteur international du secteur, « la situation est la même chez nos voisins européens, exception faite de l'Allemagne et du UK ». S. Héon nous le confirme dans son entretien[60].

S. Héon[61] précise les raisons pour lesquelles l'Allemagne et la Grande-Bretagne sont positionnées devant la France :

- En **Allemagne**, le tissu de PME, plus important, plus industriel aussi, génère une demande supérieure. Les courtiers allemands sont nombreux et investissent dans la formation sur le risque cyber. En complément, la fédération allemande de l'assurance a publié dès mars 2017 une contrat socle d'assurance cyber pour les PME[62] ;
- Au **Royaume-Uni**, le dispositif des « *cyber essentials* »[63] existe depuis 2014 : les PME doivent obligatoirement disposer de ces certifications pour pouvoir répondre à des appels d'offres publics. Peu coûteuses, ces certifications constituent un bon levier pour permettre un développement de la cyber résilience, par une liste de mesures préventives adaptées.

Au niveau mondial, deux marchés se distinguent pour leur cyber-maturité : Israël et les Etats-Unis.

L'essor de la cyber-puissance israélienne s'inscrit dans le choix des élites de privilégier une industrie du savoir dès les années 1990 et de sécuriser le pays par une armée forte. Ainsi, 40% des exportations manufacturées israéliennes concernent des produits de haute technologie, contre 16% pour la moyenne de la zone OCDE[64]. La « *start-up* nation » favorise la prise d'initiative dans le domaine digital, à Tel-Aviv notamment, où l'on voit concrètement fleurir des écosystèmes favorisant les

[58] EIOPA, communiqué de presse "*EIOPA launches survey on access to cyber insurance by SMEs*", 20 septembre 2023
[59] Marie-Ève Michelon, directrice de la souscription Europe chez Beazley Digital citée dans L'Argus de l'assurance, "Risque cyber : pourquoi les PME ne s'assurent (toujours) pas", 28 juin 2023
[60] Sébastien Héon, *Deputy Chief Underwriting Officer – Cyber Solutions,* Scor, entretien du 1er février 2023
[61] Sébastien Héon, *Deputy Chief Underwriting Officer – Cyber Solutions,* Scor, entretien du 1er février 2023
[62] Equivalent de France Assureurs en Allemagne, le *Gesamtverband der Versicherer (GDV)* a notamment créé le programme *Cybersicher, https://www.gdv.de/gdv/themen/digitalisierung/initiative-cyber-sicher*
[63] *www.gov.uk/government/publications/cyber-essentials-scheme-overview*
[64] JC. Noël, « La Cyberpuissance israélienne : l'essor inachevé de la start up nation ? », IFRI, novembre 2020

interactions entre entreprises et universités. Israël a par ailleurs été le premier pays à se doter d'un numéro d'appel d'urgence 24/24-7/7 pour les victimes de cyberattaques[65] et à avoir instauré des cours de cybersécurité dès le collège[66].

Aux Etats-Unis, le marché affiche un degré de maturité plus élevé, avec un montant de primes directes en 2022 de 7,2 Md$[67]. Deux raisons l'expliquent :

- La réglementation sur la protection des données personnelles, très puissante (et plus ancienne que la réglementation européenne) expose les entreprises à un risque de réputation et de contentieux important. En cas de sinistre, ce risque peut entraîner de possibles *class actions*. Ainsi, en plus de la garantie dommages, c'est le volet responsabilité civile qui soutient la croissance du marché ;
- Les différences culturelles : selon Inquest[68], les assureurs américains se posent "culturellement" moins de questions sur la rentabilité à court terme, s'inscrivant davantage dans une logique de "*test and learn*" pour améliorer progressivement leurs offres.

Conclusion partielle

Le poids des PME au sein de l'économie française est significatif ; elles représentent au niveau national près de 50% des emplois et plus de 40% de la valeur ajoutée.
Le risque cyber a évolué de façon matérielle ces dernières années. La cybercriminalité connaît un essor continu, porté par le développement de solutions à faible coût qui visent des attaques massives. Dans ce contexte, une cyberattaque sur deux en France aurait visé les PME, alors même que le marché de l'assurance-cyber en reste à des débuts balbutiants et focalisés sur les grandes entreprises.
La situation française ne fait pas figure d'exception à l'échelle européenne (même si l'Allemagne et le Royaume-Uni sont plus avancés) ou au niveau international (à l'exception d'Israël et des Etats-Unis qui démontrent un degré plus avancé de cyber-maturité).

[65] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises « La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ? », juin 2021
[66] Sécurité et Défense magazine, « Tour du monde de la sécurité : des approches diverses », 15 juin 2023
[67] AM Best, "*Market Segment Report: US Cyber: First Hard Market Cycle Brings a Return to Profitability*", 13 juin 2023
[68] Christophe Arrebolle, Président et Alexis Nardone, Directeur général, INQUEST, entretien du 8 mars 2023. Inquest est un acteur de référence dans la gestion des sinistres cyber

2. Les évolutions récentes du marché français : multiplication des initiatives liées au risque cyber et développement du marché de l'assurance cyber

Cette section s'attache à décrire les évolutions récentes du marché français concernant le risque cyber : nous décrirons les nombreuses initiatives des acteurs publics et professionnels de ces dernières années et nous nous attarderons sur les développements du marché de l'assurance cyber.

En premier lieu, nous notons les **multiples initiatives récentes des organisations professionnelles et des pouvoirs publics pour accompagner les PME sur le chemin de la cybersécurité** mais aussi leur **caractère atomisé** et leur **impact globalement limité**.

Ainsi, les **organisations professionnelles ont mis en place plusieurs mesures** afin de soutenir leurs adhérents, mais **sans coordination globale**.

En matière de représentation syndicale et professionnelle, la confédération des petites et moyennes entreprises (CPME) se classe comme la première organisation patronale française en nombre d'adhérents (243 000 entreprises employant plus de 4M de salariés)[69]. Le MEDEF arrive en seconde position, avec ses 190 000 entreprises adhérentes représentant 10,8M d'employés[70].

Ces deux organisations ont fortement investi le sujet du cyber et activent de nombreux leviers, notamment via leurs commissions numériques.

Pour aider les PME à se protéger des cyberattaques, la CPME a notamment contribué à la publication d'un guide pratique de l'ANSSI en février 2021[71], qui propose un accompagnement pas à pas en cybersécurité. Elle a également mis en ligne sur son site une assistance cyber, en partenariat avec cybermalveillance.gouv.fr, pour venir en aide aux victimes d'attaques : il s'agit d'un *chatbot* qui diagnostique gratuitement le problème rencontré et prodigue des conseils pour y remédier.

Les fédérations professionnelles collaborent pour mettre en œuvre des mesures prophylactiques et diffuser des bonnes pratiques face aux risques encourus : l'U2P[72], le MEDEF et la CPME ont ainsi élaboré en 2021, en lien avec le secrétariat d'Etat chargé de la transition numérique, le dispositif

[69] France Num (portail de la transformation numérique des entreprises), www.francenum.gouv.fr/partenaires/
[70] France Num (portail de la transformation numérique des entreprises), www.francenum.gouv.fr/partenaires/
[71] ANSSI, "La Cybersécurité pour les TPE/PME en 12 questions", février 2021
[72] Union des Entreprises de Proximité

« Alerte Cyber »[73], qui informe rapidement les PME en cas de failles de sécurité majeures pouvant affecter leur activité.

Toutefois, selon le dernier baromètre réalisé par l'Ifop pour Fiducial, 54% des patrons des très petites entreprises ont une mauvaise image des organisations patronales interprofessionnelles, en particulier du MEDEF[74]. Cet élément pourrait nuire à l'impact du message et des actions vers les PME.

Les Chambres de Commerce ont également mis en œuvre des dispositifs d'accompagnement, de recommandation ou de certification[75]. CCI France a ainsi créé en 2018 son réseau de formation « Initiative Data Compétences » et une certification de « référent cybersécurité en PME », permettant à l'entreprise de se doter d'un véritable « sauveteur secouriste cybersécurité ».

En second lieu, l**es pouvoirs publics à l'échelle nationale et européenne ont eux aussi multiplié les initiatives en faveur de la cybersécurité**.

Conscient de l'importance cruciale de garantir la résilience de notre pays face à la menace, le Président Macron a annoncé une **stratégie d'accélération pour la cybersécurité en janvier 2021**, financée à hauteur d'1Md€ par le plan France 2030. Dans ce cadre, l'ambition du Chef de l'Etat est de soutenir la croissance de l'industrie française de la cybersécurité, et de faire émerger des leaders aptes à renforcer la souveraineté du pays sur des technologies stratégiques.

C'est tout le sens de la **création du Campus Cyber**, inauguré en février 2022 : ce lieu totem vise à renforcer les synergies entre acteurs publics et privés.

Dès 2008, la menace cyber a été prise en compte par le gouvernement dans le livre blanc sur la défense et la sécurité nationale. Elle l'a conduit à renforcer significativement les capacités nationales en matière de cyberdéfense. La **création** de l'Agence nationale de la sécurité des systèmes d'information (**ANSSI**), en juillet 2009, marque la première étape de cet engagement. L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. Centrée en priorité autour de la sécurité des systèmes d'informations de l'État et des opérateurs stratégiques, l'ANSSI mène également des actions de proximité en région dans le but d'assister les collectivités territoriales et les PME. Elle a notamment mis en place 12 équipes régionales de réponse aux incidents informatiques

[73] Gouvernement, communiqué de presse "Cédric O présente le nouveau dispositif d'alerte des entreprises en cas d'incident majeur", 20 juillet 2021
[74] Sondage Ifop pour Fiducial réalisé auprès de 1 001 dirigeants de PME de 0 à 19 salariés réalisant plus de 50 000 euros de chiffre d'affaires cité dans Les Echos, "Les très petites entreprises ont une mauvaise image des organisations patronales nationales", 26 juin 2023
[75] CCI Ile de France, "Pérenniser l'entreprise face au risque cyber", juin 2021

(CSIRT[76]). Par ailleurs, Les MOOC de l'ANSSI sur la cybersécurité sont reconnus comme des outils d'une "extrême utilité[77]".

Les PME qui ont un lien avec des questions d'intelligence économique peuvent être plus ciblées que d'autres par des cyberattaques. Pour les aider, le gouvernement a lancé fin 2022 un dispositif d'accompagnement financier visant 750 d'entre elles : les premières candidatures des entreprises éligibles ont été déposées durant l'été 2023.

En complément, **BPI France** a lancé en mars 2023 son "**DiagSécurité**"[78], un diagnostic de cybersécurité dédié aux PME. BPI France finance 50% de l'audit, soit un reste à charge de 2 200 € pour l'entreprise.

Au niveau européen enfin, l'heure est à la construction de règles visant à atteindre les mêmes objectifs de régulation et de sécurisation de l'espace numérique. Sous l'égide du commissaire Thierry Breton, de nombreuses initiatives sont en cours : directive NIS2, règlement *Cyber Resilience Act*, projets de règlements sur un portefeuille européen d'identités numériques ou *AI* Act.

En particulier, la **directive NIS2**, adoptée en novembre 2022, a pour objectif d'étendre les exigences en matière de cybersécurité à un nombre plus important de secteurs sensibles et aux entités employant plus de 50 personnes. Son entrée en vigueur, attendue d'ici octobre 2024[79], devrait se traduire par une **multiplication par dix du nombre d'entités entrant dans le périmètre de contrôle de l'ANSSI[80]**.

Après cette revue des différentes initiatives en faveur de la cybersécurité prises par les acteurs professionnels et public, nous nous focalisons désormais sur le marché de l'assurance cyber en France, caractérisé par la **construction progressive d'une offre d'assurance cyber qui implique de multiples acteurs de la profession**.

L**'assurance couvrant spécifiquement le risque cyber** existe depuis 2000. Les premières polices ont été conçues pour le marché des *Lloyd's* de Londres : elles prévoyaient une couverture en

[76] *Computer Security Incident Response*
[77] CESE, "Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques", avril 2022
[78] BPI France, communiqué de presse « Cybersécurité : "Bpifrance poursuit son ambition d'accompagner les entreprises dans la prévention de ce risque et lance le « Diag Cybersécurité » », 20 mars 2023
[79] ANSSI, https://www.ssi.gouv.fr/directive-nis-2/
[80] Institut Montaigne, "Cybersécurité : passons l'échelle", juin 2023

responsabilité civile ainsi qu'une couverture contre les interruptions d'activité, pour les dommages ayant un rapport de causalité avec un antécédent cybercriminel.

Cette offre s'est étendue au niveau international, dont le marché français. Actuellement, à l'exception notable d'Axa, les **principaux acteurs** sont **anglo-saxons** et disposent d'une **expertise spécifique sur le risque cyber** : Chubb, AIG, Hiscox ou Beazley sont les leaders sur ce marché. Le premier assureur à réellement avoir cherché à démocratiser l'assurance cyber de PME a été Hiscox, à partir de 2008[81].

Les **principales garanties offertes par les polices d'assurance cyber** sont les suivantes :

- Frais et pertes subis à la suite d'une intrusion malveillante (dommage) :
    - Expertise IT ;
    - Frais de gestion de l'incident et frais de gestion de crise ;
    - Frais de reconstitution des données ;
    - Frais de réparation du ou des système(s) infecté(s) ;
    - Pertes d'exploitation consécutives ;
- Frais liés à une violation de données personnelles, frais d'enquête administrative et de notification ;
- Conséquences en termes de responsabilité civile :
    - Dommages aux tiers liés à un défaut de sécurité ;
    - Frais d'avocat et de défense.

En complément, les assureurs proposent souvent un **panel de services** plutôt orientés vers l'accès à des experts en cybersécurité et/ou des professionnels de la gestion de crise pour offrir des services de **prévention** et d'**assistance** en cas de cyber incident. Hiscox a ainsi par exemple développé un outil d'évaluation de l'exposition aux cyber-risques pour sa clientèle de PME.

En parallèle de ce développement d'une offre d'assurance dédiée au risque cyber, **il subsiste dans les polices dites "traditionnelles"** des ambiguïtés sur la couverture (ou non) des sinistres d'origine cyber qui sont à l'origine du problème **des "garanties silencieuses"**. Cette situation n'est pas isolée à la France puisque l'EIOPA a une nouvelle fois demandé une clarification générale des pratiques en 2022[82].

[81] Franck Lourdelet, Responsable Partenariats Hiscox France, entretien du 6 juillet 2023
[82] EIOPA, "*Consultation paper on supervisory statement on management of non-affirmative cyber underwriting exposures"*, mai 2022

Des contrats "traditionnels" d'assurance peuvent en effet contenir des niveaux de garantie implicites, susceptibles de couvrir certaines conséquences des dommages liés au numérique : les contrats de **responsabilité civile** pour des dommages aux tiers, matériels et corporels, des dommages consécutifs, des frais de justice ou encore la responsabilité des mandataires sociaux. Des garanties cyber peuvent également figurer dans les contrats assurant les **dommages aux biens.** Ces derniers peuvent être activés dans certaines situations, pour couvrir des dommages matériels sur des marchandises ou des locaux professionnels, des pertes d'exploitation ou encore des frais de justice.

En cas d'incident cyber avec des répercussions systémiques, les conséquences pourraient ainsi être désastreuses pour la solvabilité des assureurs et des réassureurs, faute de provisionnement adapté en lien avec ces clauses préexistantes à la possibilité d'une crise numérique majeure.

Concrètement, le marché français est donc partagé entre :

- Une offre dédiée au risque cyber, dotée de garanties claires, mais pénalisée par un manque de maturité et de mutualisation ;
- Des garanties silencieuses qui freinent le développement de l'assurance cyber devant la difficulté pour les assureurs à mesurer leur exposition totale actuelle au risque cyber.

Nous focalisons désormais notre analyse du marché français sur les **réassureurs** qui jouent un rôle clé dans l'écosystème de l'assurance cyber, car **les cédants leur confient autour de 55% de leur risque à l'échelle mondiale et plus de 60% en EMEA**[83]. Selon S. Héon, le taux sur le marché français atteindrait jusqu'à 65% ou 70%. La réassurance proportionnelle domine nettement : 87% selon S&P[84].

Les réassureurs adoptent une approche globale de leurs portefeuilles et leur modèle consiste à mutualiser les risques souscrits sur le plan international. Le caractère systémique du risque les expose à un risque de cumul important. Ils préfèrent donc couvrir des garanties affirmatives (non silencieuses), avec une analyse approfondie des portefeuilles cédés. Au regard du faible taux de pénétration de l'assurance cyber pour les PME en France, les réassureurs manquent de données et d'expertise en la matière.

[83] *S&P, "Global Cyber Insurance : Reinsurance Remains Key to Growth",* août 2023 - EMEA signifie *Europe, Middle East and Africa*
[84] *S&P, "Global Cyber Insurance : Reinsurance Remains Key to Growth",* août 2023

Ce panorama du marché français ne serait pas complet sans mentionner le **rôle émergent des *insurtech***.

Face à un marché de l'assurance cyber avec de fortes perspectives de développement, les *insurtech*, fortes du constat du manque d'adaptation des solutions proposées par les assureurs traditionnels aux PME, tentent d'apporter une **réponse innovante et pragmatique** sur le marché de l'assurance cyber.

Dattak, MGA créé en 2021[85], a choisi d'accompagner plus spécifiquement les PME, avec Wakam comme preneur de risque. Elle propose des solutions d'assistance et d'assurance. Elle y adjoint des innovations, telles qu'un parcours de souscription en quatre questions et 100% digital, ainsi qu'un « *cyber scan* » capable d'identifier les failles IT du client. Les services associés au contrat comportent une formation continue à la cybersécurité et des attaques inopinées de type « phishing », afin de sensibiliser les collaborateurs[86]. Stoïk a également développé une offre sur un positionnement similaire en s'appuyant sur un assureur (Acheel) et un réassureur (SwissRe).

Conclusion partielle

En France, les initiatives visant à développer la sensibilisation au risque cyber des PME et à les accompagner se multiplient au sein des acteurs privés et publics mais elles sont en ordre dispersé.
Le marché de l'assurance cyber se développe progressivement, porté majoritairement par des assureurs anglo-saxons disposant d'une expertise avancée dans ce domaine.
En parallèle, le sujet des garanties silencieuses incluses dans les polices traditionnelles reste d'actualité.
Certaines *insurtech*, comme Dattak, ont développé des offres innovantes dédiées aux PME, qui allient diagnostic de cybersécurité, mesures de prévention et couverture assurantielle.

[85] *Managing General Agent*
[86] Charlotte Couallier, CEO de Dattak, entretien du 13 janvier 2023

B. Des PME marginalement couvertes contre le risque cyber : analyse des freins et blocages

Nous avons établi plus haut que, bien que très exposées au risque cyber, les PME ne sont que marginalement couvertes par une assurance. Dans cette section, nous analyserons en détail les différents freins et blocages, aussi bien du côté de la demande que de l'offre, qui conduisent selon nous à cette situation. Pour finir, nous verrons que l'écosystème contribue également à ces freins et à ces blocages.

1. Les freins et les blocages pour les PME

La **sous-estimation du risque cyber par les PME** constitue selon nous le premier frein qui explique la situation actuelle.

L'Étude OpinionWay[87] pour QBE sur la gestion des risques des PME et des ETI en France illustre la sous-évaluation du risque cyber :

- Seuls 20% des dirigeants d'entreprise considèrent que leur entreprise fait face au risque d'une cyberattaque ;
- 83% d'entre eux pensent que leur entreprise est capable de gérer une cyberattaque.

Ces constats sont confirmés par une récente étude de la Fédération Française de la Cybersécurité[88] menée auprès de plus de 500 PME : un tiers des entreprises interrogées ne se considèrent pas comme une cible potentielle pour les hackers. Elles étaient 70% en 2021, ce qui démontre à la fois une nette amélioration et un contrat qui reste préoccupant.

Le degré de prise de conscience semble inversement corrélé au niveau de "cyber-maturité" : selon Hiscox[89], 58% des entreprises "cyber-expertes" estiment que leur risque d'exposition à une attaque est élevé, contre seulement 32% parmi les "cyber-novices".

Il est également probable que les dirigeants de PME sous-estiment les coûts et les impacts liés à une cyberattaque. Comme le souligne l'étude menée par le cabinet Bessé avec Stelliant[90], de nombreuses

[87] OpinionWay pour QBE, "Gestion des risques des PME et ETI en France", 6ème édition, février 2023. 302 participants dont 92% représentent des PME
[88] Fédération Française de la Cybersécurité (en partenariat avec Apave, Itrust et Free Pro), "Enquête de maturité des TPE/PME françaises 2023", juillet 2023
[89] Hiscox Assurances, "Rapport 2022 sur la gestion des cyberrisques", 6ème édition, novembre 2022
[90] Bessé, en partenariat avec Stelliant, "Risques cyber : analyse de la sinistralité : quels enseignements ?", octobre 2022. Les TPE et PME représentent 56% des sinistres analysés

entreprises sous-évaluent le délai de retour à la normale et surestiment leur capacité à retrouver rapidement un niveau normal d'activité.

Aux coûts directs liés à l'attaque, il faut souvent ajouter les dépenses liées à la reconstitution des données ou de tout ou partie d'un système d'information (dans 94% des cas pour les victimes)[91] et, parfois, les frais liés à l'engagement de la responsabilité civile.

Les dirigeants de PME, qui sont souvent sous-traitants ou partenaires de grandes entreprises **minorent** également **le risque de mise en cause de leur responsabilité** personnelle. En effet, un dispositif insuffisant de cybersécurité pourrait donner lieu à une procédure pour faute par abstention[92]. Ce risque est renforcé par une loi de 2017 relative au devoir de vigilance des sociétés donneuses d'ordre[93], qui impose aux grandes entreprises un contrôle des sous-traitants, notamment en matière de cyber risque. "La cybersécurité est donc aussi, et de plus en plus, un risque juridique"[94].

En résumé, comme le résume cette citation, la plupart des PME "n'ont toujours pas conscience du risque qu'elles encourent, c'est-à-dire, très concrètement, de l'impossibilité de surmonter la perte financière et d'image engendrée par l'attaque"[95].

Le deuxième frein que nous identifions réside dans le manque de moyens des PME pour se prémunir face au risque cyber. Alors que les OIS (opérateurs d'importance vitale) sont protégés de manière satisfaisante par l'ANSSI, les PME ne bénéficient pas de ce dispositif public[96].

Les PME françaises :

- Ont généralement des connaissances faibles en informatique et une **culture de gestion des risques peu développée**, même si les entreprises sont mieux organisées à la suite de la pandémie[97] ;
- **Disposent rarement de collaborateurs dédiés aux systèmes d'information**, encore moins à leur sécurité[98] ;

[91] Bessé, en partenariat avec Stelliant, "Risques cyber : analyse de la sinistralité, quels enseignements ?", octobre 2022. Les TPE et PME représentent 56% des sinistres analysés
[92] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[93] Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre
[94] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[95] Le Club des Juristes, "Le Droit pénal à l'épreuve des cyberattaques", avril 2021
[96] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[97] CESE, "Climat, cyber, pandémie : le modèle assurantiel mis au défi des risques systémiques", avril 2022
[98] Allianz, Axa, HDI, Howden, Marsh, Lloyds, MunichRe, FERMA "*How Can Europe Lead the Way to Cyber Resilience*", juin 2023

- Sont davantage exposées au manque de formation cyber des collaborateurs et à la prise de conscience des dangers des cyberattaques[99].

L'étude récente de la Fédération Française de la Cybersécurité sur les PME françaises[100] confirme ces constats :

- 61% des entreprises interrogées n'ont aucune ressource dédiée à la cybersécurité ;
- 47% des entreprises n'ont aucun document cyber au sein de leur structure (charte informatique, plan de continuité ou de reprise d'activité…).

Comme le note Jérôme Notin, Directeur Général du GIP ACYMA (qui gère le dispositif de cybermalveillance.gouv.org), une très grande majorité des cyberattaques pourrait être évitée avec la **mise en place de mesure "d'hygiène" cyber** : gestion des mots de passe, installation des mises à jour de sécurité, sauvegarde régulière des données[101]… En l'absence de collaborateur dédié, cette rigueur informatique est plus difficile à maintenir.

Selon un sondage réalisé par le Cyber Readiness Institute[102] auprès de 14 000 PME dans le monde, 55% des entreprises n'ont pas encore mis en place une authentification multi-facteur, une mesure basique d'hygiène informatique. En complément, l'étude de la Fédération Française de la Cybersécurité déplore que près de 40% des entreprises interrogées n'aient pas de politique de sécurité concernant les appareils mobiles et que plus de la moitié de celles qui mettent leur réseau *Wi-FI* à disposition des visiteurs le fassent de manière non sécurisée.

En outre, les PME ont une architecture IT qui les expose particulièrement :

- **La majorité des PME ont recours à des services *cloud* mais avec une faible maîtrise des enjeux techniques** et dans le cadre d'une relation commerciale déséquilibrée (certains prestataires refusant toute responsabilité en matière de disponibilité ou de fonctionnalité du service, contrairement aux pratiques observées auprès des grandes entreprises)[103]. Cette situation est renforcée par le poids des trois premiers acteurs du *cloud* qui représentent plus de 65% de part de marché[104] ;

[99] FERMA, "*Position Paper on the European Commission's Cyber Resilience Act Initiative*", mai 2022
[100] Fédération Française de la Cybersécurité (en partenariat avec Apave, Itrust et Free Pro), "Enquête de maturité des TPE/PME françaises 2023", juillet 2023
[101] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[102] The Wall Street Journal, *"Smaller Companies Are Urged to Adopt Multifactor Authentification"*, 5 juillet 2022
[103] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[104] Allianz, "*Cyber : The Changing Threat Landscape*", octobre 2022

- En général, les PME se concentrent sur un nombre limité d'outils externes et d'applicatifs : en conséquence, elles exercent un faible degré de contrôle sur leur niveau de cybersécurité qui dépend essentiellement de celui de leurs prestataires[105] ;
- **Les outils et applicatifs achetés et utilisés par les PME n'intègrent pas la cybersécurité par défaut[106],** leur laissant cette responsabilité alors qu'elles sont peu équipées pour évaluer la cybersécurité des solutions envisagées et qu'elles ne peuvent s'appuyer sur des standards partagés de sécurité minimale.

Par ailleurs, le **contexte économique** de ces dernières années (pandémie, inflation) **a pu contraindre les dépenses de cybersécurité des PME.** Selon Marc Bothorel[107], le budget représente un jour de chiffre d'affaires pour une petite structure.

En complément de ce manque de moyens, certains **dirigeants de PME** ont parfois une mauvaise compréhension de leurs polices d'assurance et **pensent (à tort ou à raison) être déjà couverts contre le risque cyber**, via leurs polices de responsabilité civile et de dommages aux biens.

Certes, des exclusions ou garanties explicites ont été progressivement introduites ces dernières années, mais les pratiques demeurent hétérogènes et concernent principalement le flux de nouveaux contrats[108]. Pour illustrer ce phénomène, une étude de l'AGEA[109] (fédération nationale des syndicats d'agents généraux d'assurance) sur les contrats commercialisés en 2021 constate que, sur 11 contrats étudiés, trois n'excluent pas clairement le risque cyber. Cette étude est particulièrement pertinente dans la mesure où les PME constituent une clientèle privilégiée pour les agents généraux d'assurance.

L'ACPR confirme que l'ambiguïté n'a pas disparu en invitant à deux reprises ces dernières années les assureurs "à clarifier et à rendre plus explicites les formulations des termes et conditions des polices en ce qui concerne la couverture ou l'exclusion des risques cyber"[110].

Ainsi, la conclusion de ce rapport du Club des Juristes de 2018[111] reste, au moins partiellement vraie pour les PME : "la complexité et l'opacité des couvertures cyber atomisées entre plusieurs types de contrats d'assurance dissuadent souvent de souscrire une assurance cyber".

[105] Allianz, Axa, HDI, Howden, Marsh, Lloyds, Munich Re, FERMA, *«How Can Europe Lead the Way to Cyber Resilience*", juin 2023
[106] Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018
[107] Marc Bothorel, Référent national cybersécurité pour la CPME, entretien du 1er juin 2023
[108] Direction Générale du Trésor, "Le Développement de l'assurance du risque cyber", septembre 2022
[109] Étude citée dans le rapport de la Direction Générale du Trésor, "Le Développement de l'assurance du risque cyber", septembre 2022
[110] ACPR, communiqué de presse "Garanties implicites contenues dans les contrats en matière de couverture du risque cyber", 23 septembre 2022, qui fait suite au communiqué de presse du 12 novembre 2019 "La Distribution des garanties contre les risques cyber par les assureurs"
[111] Le Club des Juristes, "Assurer le risque cyber", janvier 2018

Par ailleurs, l'**assurance cyber** reste **méconnue des dirigeants des PME**, ce qui constitue un autre blocage expliquant la situation actuelle.

Une étude de Munich Re[112] (menée au niveau mondial) illustre ce frein à la souscription. Parmi les entreprises qui n'ont pas souscrit d'assurance cyber, 25% des participants répondent qu'ils n'ont pas connaissance de cette offre. Ce pourcentage augmente à 38% pour les sociétés dont le chiffre d'affaires annuel est inférieur à 1 M$.

Quand les dirigeants de PME s'intéressent à la souscription d'une assurance cyber, ils sont souvent rebutés par la **difficile comparaison des offres**.

Au-delà du problème de chevauchement de l'assurance cyber avec les autres polices d'assurances des PME, les offres d'assurance cyber manquent d'harmonisation : **les définitions, la terminologie, les garanties, limites et exclusions varient d'un assureur à l'autre**[113], ce qui freine la souscription. A titre illustratif, la définition du système d'information varie selon les assureurs et inclut ou non les systèmes d'un partenaire cloud[114].

Le processus de souscription renforce la complexité perçue. Les **questionnaires de cybersécurité** des assureurs ne sont ni harmonisés, ni adaptés à la taille ou aux spécificités des entreprises. Ils représentent une charge administrative significative pour les PME. En l'absence d'un directeur des systèmes d'information, le dirigeant se trouve souvent désarmé pour répondre[115].

Comme le note la *regtech*[116] néerlandaise ISUNA[117], le niveau de détail de la *due diligence* des assureurs constitue un obstacle unique à l'accès au marché de l'assurance cyber.

Enfin, **le rapport "qualité/prix" de l'assurance cyber peine à convaincre les dirigeants de PME**.

Les **limites et exclusions imposées par les assureurs** contribuent à réduire la valeur perçue de l'assurance cyber. Le sentiment des dirigeants est qu'ils sont face à un **marché d'offre**, où les

[112] *Munich Re, "Global Cyber Risk and Insurance Survey 2022",* août 2022
[113] OCDE, *"Enhancing the Role of Insurance Cyber Risk Management",* novembre 2017
[114] Le Club des Juristes, "Assurer le risque cyber", janvier 2018
[115] Direction Générale du Trésor "Le Développement de l'assurance du risque cyber", septembre 2022
[116] Une *regtech* est une entité innovante qui utilise les nouvelles technologies pour faciliter la conformité aux exigences réglementaires
[117] ISUNA, *White Paper "Cyber Insurance: Multistakeholder Challenges and Solutions*", septembre 2022

couvertures dépendent davantage du niveau de risque que les assureurs sont prêts à prendre, que de leurs besoins de protection[118].

En complément, pour accéder à l'assurance cyber, les entreprises doivent souvent consentir, en amont de la souscription, des **investissements en cyber sécurité**. Ces standards de cybersécurité requis par les assureurs peuvent être perçus comme inatteignables par certaines structures de taille modeste[119].

Bien que ces investissements permettent d'entrer dans un cercle vertueux (meilleur dispositif de cybersécurité et couverture assurantielle), le coût global constitue clairement un frein à la souscription pour les dirigeants de PME. Selon un témoignage d'un agent général[120], même en proposant des solutions d'*insurtech* souples et simplifiées, le coût de l'assurance demeure un frein majeur pour les dirigeants de PME.

Les évolutions du marché de l'assurance cyber ces dernières années (augmentation des prix cumulée à une réduction des garanties) ne font que renforcer cette faible attractivité, notamment pour les petites structures[121] [122].

Conclusion partielle

Le faible degré de cyber-maturité des PME peut s'expliquer par de nombreux facteurs : une sous-estimation du risque cyber qui reste significative, un manque de moyens financiers et humains pour se prémunir du risque cyber et pour comprendre des offres assurantielles qui manquent de clarté et sont peu adaptées aux PME.
Comme mentionné dans un rapport de l'Assemblée Nationale, les entreprises les plus modestes sont "démunies, tant techniquement que juridiquement face aux cyber agressions"[123]. En comparaison avec les grands groupes[124] :

- Elles disposent de moins de ressources financières (pour investir en cybersécurité et/ou s'assurer) ;
- Leur pouvoir de négociation (face aux prestataires IT ou aux assureurs) est réduit.

[118] OCDE, "*Unleashing the Potential of the Cyber Insurance Market*", février 2018
[119] OCDE, "*Unleashing the Potential of the Cyber Insurance Market*", février 2018
[120] F. Prissé, agent général MMA, entretien du 21 septembre 2023
[121] ENISA, "*Demand Side of Cyber Insurance in the EU*", février 2023. Étude menée auprès de plus de 260 Opérateurs de Service Essentiel dans 25 pays européens dont près de 30% emploient moins de 250 salariés.
[122] AMRAE, "Etude LUCY" (LUmière sur la CYberassurance), 2ème et 3ème éditions, juin 2022 et mai 2023
[123] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[124] CESE, "Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques", avril 2022

2. Les freins et les blocages pour les acteurs du secteur de l'assurance

Du côté des assureurs, le **risque cyber** est considéré comme **difficile à modéliser, tarifer et mutualiser**, ce qui le place **à la limite de l'assurabilité**.

L'assurabilité du risque cyber a donné lieu ces dernières années à la publication de nombreux articles et travaux de recherche[125]. Ces travaux analysent notamment l'assurabilité du risque cyber à l'aune des neuf critères d'assurabilité de Berliner[126].

Le risque cyber pose des défis évidents en termes d'assurabilité, notamment compte tenu de l'asymétrie d'information (et de l'aléa moral qui en découle), de la dimension systémique de ce risque (renforcée par l'interconnexion des systèmes d'information), de son caractère évolutif et de l'historique limité dont disposent les assureurs. Ces défis s'ajoutent à une incertitude sur le niveau réel des garanties données (et donc de l'exposition aux pertes), compte tenu des garanties silencieuses. Ces limites à l'assurabilité sont renforcées par la faible profondeur du marché qui limite la diversification.

Néanmoins, ces travaux portent sur le risque cyber en général et ne permettent pas, à première vue, d'expliquer la situation actuelle du marché français où **94% des grandes entreprises ont une assurance cyber** mais seulement 3% des entreprises de taille moyenne e**t 0,2% des petites entreprises**[127]. Cette situation apparaît comme paradoxale puisqu'on peut penser que les plus petites structures sont moins à même de générer des sinistres de très haute intensité.

Trois éléments nous semblent pouvoir expliquer ce paradoxe :

- **Un facteur économique** : comme mentionné précédemment, la souscription d'une analyse cyber s'accompagne d'une **"*due diligence*" technique approfondie**, qui représente u**n coût certain pour le preneur de risque**, coût qu'il est plus difficile de justifier pour une police d'un montant modeste ;
- **Un facteur technique lié au profil de cyber-maturité des PME** : comme le résume Marek Stanislawski, responsable de la souscription cyber pour AGCS, le marché dispose d'une

[125] Notamment : C. Biener, M. Eling et JH Wirfs, "*Insurability of Cyber Risks: an Empirical Analysis*", The Geneva Association et Institute of Insurance Economics at the University of St Gallen, août 2014, M. Eling et JH Wirfs, "*Cyber Risk: Too Big To Insure*", University of St Gallen et Swiss Re, 2016, OCDE *"Enhancing the Role of Insurance in Cyber Risk Management"*, novembre 2017 et S. Héon et D. Parsoire, "La Couverture du cyber risque", The Geneva Papers on Risk and Insurance, février 2017
[126] Cf Annexe 2
[127] AMRAE, "Etude LUCY" (LUmière sur la CYberassurance), 3ème édition, mai 2023. Dans l'étude, les ETI ont un chiffre d'affaires compris entre 50 M€ et 1,5 Md€ et les entreprises de taille moyenne ont un chiffre d'affaires compris entre 10 M€ et 50 M€

capacité suffisante pour les sociétés qui ont une bonne compréhension de leur profil de risque et qui ont mis en place les contrôles et les sécurisations adéquats[128]. Ce qui est une façon d'illustrer l'expression populaire "on ne prête qu'aux riches" ;

- **La jeunesse et de l'immaturité du marché** : les assureurs actifs sur le marché de l'assurance cyber en France sont peu nombreux et majoritairement anglo-saxons. On peut comprendre que ces preneurs de risque se soient focalisés sur le petit nombre de courtiers qui couvrent les grandes entreprises pour assurer leur développement rapide, en limitant leurs coûts d'acquisition des clients .

En résumé, la situation actuelle reflète la définition de l'assurabilité que MG Fauré[129] reprend à son compte : "l'assurabilité, c'est la volonté de l'assureur d'offrir une couverture".

Autre frein identifié du côté des preneurs de risque : la **volatilité de la sinistralité sur le marché français**.

L'étude LUCY[130] publiée annuellement par l'AMRAE depuis trois ans permet d'avoir un aperçu du ratio sinistres / primes des assureurs cyber :

Ratio S/P	**2019**	**2020**	**2021**	**2022**	**Moyenne**
Grandes entreprises	44%	190%	58%	16%	61%
ETI	481%	85%	261%	51%	157%
PME	nd	45%	36%	100%	67%
Moyenne marché	**84%**	**167%**	**88%**	**22%**	**73%**

Comme le montre le tableau ci-dessus, les ratios de sinistres / primes du marché français de l'assurance cyber ont été très volatiles sur les quatre dernières années.

Après la forte sinistralité observée sur le segment des grandes entreprises en 2020, les assureurs ont, comme le montre l'étude, fortement augmenté leurs niveaux de primes, réduit leurs capacités et relevé leurs franchises en 2021 sur cette clientèle. Un phénomène similaire a affecté les ETI en 2022 après

[128] *Allianz, "Cyber, The Changing Threat Landscape*", octobre 2022
[129] MG. Fauré, "*The Limits of Insurability From a Law and Economic Perspective*", The Geneva Papers on Risk and Insurance, juillet 1995
[130] Cf. Annexe 1 pour une présentation détaillée de l'étude

le pic de sinistralité de l'année 2021. Et il est probable que l'histoire se répète pour les PME en 2023 et 2024, après le niveau élevé du ratio sinistres/primes en 2022.

Malgré cette volatilité qui illustre le manque de maturité de ce jeune marché, le ratio moyen de sinistres / primes s'établit à 73% sur les quatre dernières années, en ligne avec le ratio moyen sur la même période de l'assurance de dommages aux biens (69%)[131].

Au-delà des assureurs, les autres acteurs du secteur, distributeurs comme réassureurs, contribuent également aux freins et aux blocages.

Les **distributeurs** sont souvent **désarmés face au risque cyber** et aux options possibles de couverture.
Une étude récente du *think tank* de Planète CSCA[132] conclut que 63% des courtiers ne proposent pas d'offre cyber par **manque de compétence sur ce risque**. Seuls 44% disent connaître les solutions d'assurance cyber et les acteurs de ce marché. Marc Bothorel de la CPME partage ce constat[133].

Plus inquiétant, 53% des courtiers interrogés (très majoritairement des PME) ont été visés par une cyberattaque et seul un cabinet sur deux a investi dans sa propre cybersécurité[134].

Ainsi, les agents généraux, qui ont souvent développé une connaissance fine de leurs clients, ne jouent pas pleinement leur rôle important de courroie de transmission avec les PME en ce qui concerne le risque cyber.

Face à ce risque, les **réassureurs** se trouvent dans une position encore plus inconfortable que les assureurs.

Globalement, les difficultés rencontrées par les assureurs sont encore plus aiguës pour les réassureurs. Le premier obstacle réside dans la quasi-impossible **détermination de leur exposition au risque cyber** compte tenu des "garanties silencieuses". Ainsi l'APREF considère leur élimination comme "une priorité absolue"[135]. Afin de se prémunir contre ce risque, les réassureurs ont unanimement imposé des exclusions cyber dans l'ensemble des traités de réassurance ces dernières années.

[131] France Assureurs, étude statistique "L'Assurance de dommages aux biens des professionnels en 2022", juin 2023
[132] Institut Intermédius, *think tank* de Planète CSCA, "Risque cyber : "comment les cabinets de courtage de proximité peuvent-ils s'en prémunir et conseiller leurs clients", septembre 2023
[133] Marc Bothorel, Référent national cybersécurité pour la CPME, entretien du 1er juin 2023
[134] Institut Intermédius, *think tank* de Planète CSCA, "Risque cyber : "comment les cabinets de courtage de proximité peuvent-ils s'en prémunir et conseiller leurs clients", septembre 2023
[135] APREF, note de position "Assurance et réassurance du risque cyber", décembre 2021

En complément, les réassureurs ont encore davantage besoin d'intervenir sur un marché qui a atteint une certaine taille critique, afin de faire jouer les effets de la mutualisation[136].

Enfin, la diversité des polices évoquée plus haut, combinée à la nécessité de devoir se reposer sur la *due diligence* technique des assureurs, complique encore la situation des réassureurs. Comme le note Fabian Willi, *Head Cyber EMEA* de Swiss Re[137], "aujourd'hui, chaque cédante collecte et présente les données cyber à sa manière, si bien qu'il est compliqué de comparer et de comprendre ce dont on parle".

Dans ce contexte, les réassureurs font face à des contraintes de capacité sur le marché de l'assurance cyber et les renouvellements au 1er janvier 2024 s'annoncent d'ores et déjà difficiles[138].

Conclusion partielle

Le risque cyber présente des limites certaines en termes d'assurabilité mais ceci ne permet pas d'expliquer la différence de taux de couverture assurantielle entre les grands groupes et les petites entreprises.
Pour les assureurs (très majoritairement anglo-saxons, avec une approche internationale), les grands groupes présentent un degré supérieur de cyber-maturité et offrent des potentiels de primes supérieurs, permettant d'amortir le coût de la *due diligence* technique. En comparaison, les PME sont jugées comme des cibles peu attractives.
En complément, les distributeurs manquent de connaissance sur le risque cyber, les empêchant de jouer pleinement leur rôle d'interlocuteur privilégié sur ces sujets.
Enfin, dans ce marché encore jeune, le recours à la réassurance demeure massif, ce qui génère des contraintes de capacité pour les réassureurs.

3. Les freins et les blocages de l'offre et de la demande accentués par l'écosystème

[136] *Long Finance, "Promoting UK Cyber Prosperity : Public-Private Cyber Catastrophe Reinsurance",* juillet 2015
[137] L'Argus de l'Assurance, "Les réassureurs avancent à l'aveugle sur le cyber", 11 octobre 2023
[138] L'Argus de l'Assurance, "Les réassureurs avancent à l'aveugle sur le cyber", 11 octobre 2023

L'**environnement juridique et réglementaire manque de clarté sur certains aspects**, ce qui a ralenti et continue de ralentir le développement du marché de l'assurance cyber.

On peut notamment citer trois éléments sujets à débat :

- La légalité de la couverture des paiements de rançons ;
- La légalité de la couverture du paiement des sanctions administratives ;
- La définition de la cyber-guerre.

Le premier point a certes été clarifié par la loi LOPMI[139], entrée en vigueur cette année. Mais ces incertitudes juridiques ont freiné l'extension du marché vers des entreprises de taille plus modeste.

En complément, les autorités européennes ont adopté plusieurs directives visant à renforcer la cybersécurité des OIV et des OES (Directives NIS et NIS2) ou celle du secteur financier (règlement DORA) mais **aucun dispositif visant la cybersécurité des PME n'est inscrit à l'agenda de la Commission Européenne**[140].

Parmi les facteurs qui participent à la mise sous tension de la situation, nous pouvons citer l'**environnement de cybersécurité** et notamment trois éléments :

- L'**absence de standards de cybersécurité**, clairement définis et acceptés par les intervenants de marché : cette situation contribue à la lourdeur du processus de *due diligence* technique ;
- Une **menace cyber** qui **évolue très rapidement**, notamment avec une utilisation croissante de l'IA, ce qui rend tout dispositif de cybersécurité rapidement caduque ;
- Le **manque de ressources humaines en cybersécurité**, phénomène observé en France et dans le monde entier. En France, les métiers de la cybersécurité sont les plus tendus des métiers du numérique[141]. Au niveau international, 70% des entreprises déclarent ne pas avoir suffisamment de ressources humaines dans le domaine de la cybersécurité[142] ;

Mécaniquement, les entreprises de taille modeste sont celles qui pâtissent le plus de cette situation[143]. Par ailleurs, le label "CyberExpert", créé par l'ANSSI en 2021, bénéficie à ce stade d'un succès relatif avec un peu plus de 200 experts labellisés à fin 2022.

[139] Loi d'Orientation et de Programmation du ministère de l'Intérieur entrée en vigueur en avril 2023. Elle conditionne le droit à une indemnisation assurantielle à un dépôt de plainte dans un délai de 72 heures
[140] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[141] Institut Montaigne, "Mobiliser et former les talents du numérique", mai 2023
[142] Allianz, "*Cyber security trends 2023*", octobre 2023
[143] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021

Enfin, la France dispose d'un **écosystème d'acteurs publics et professionnels riche mais éclaté et doté de peu de moyens.**

Comme évoqué plus haut, plusieurs acteurs publics interviennent dans le domaine de la cybersécurité des entreprises (sans inclure les services dédiés à la cybercriminalité qui sont, eux aussi, nombreux) :

- L'ANSSI (rattachée au secrétariat général de la défense et de la sécurité nationale qui dépend du Premier Ministre) ;
- Plusieurs ministères (notamment économie, intérieur, défense, justice) ;
- Le ComCyberGend (Commandement de la gendarmerie dans le cyberespace) ;
- Le GIP ACYMA qui regroupe les acteurs publics ainsi que des acteurs privés (62 membres[144]) et gère le dispositif de cybermalveillance.gouv.fr ;
- Le Campus Cyber, inauguré en février 2022, qui a vocation à réunir les principaux acteurs cyber nationaux et internationaux ;
- Les chambres consulaires (commerce & industrie, artisanat, agriculture) ;
- Les collectivités locales.

Il convient d'ajouter à cette liste les associations professionnelles comme la CPME et celles dédiées à l'assurance (France Assureurs, AGEA…).

Les acteurs publics ne recueillent qu'une partie minime des attaques de cybersécurité :

- L'ANSSI a été notifiée de 831 incidents de cybersécurité en 2022 (vs 1057 incidents en 202)[145] ;
- En 2022, le site cybermalveillenace.gouv.fr déclare 3,8M de visiteurs uniques en 2022[146] (à titre de comparaison, le site Leboncoin totalise 27M de visiteurs uniques par mois[147]) et a reçu 280 000 demandes d'assistance, dont 6% seulement proviennent des entreprises[148].

Enfin, bien que ces acteurs (notamment l'ANSSI et le GIP ACYMA) aient développé des initiatives unanimement saluées (comme les MOOC de cybersécurité ou l'outil d'auto-évaluation de cybersécurité), les budgets alloués à ces entités restent limités :

- Mise en place de 12 CSIRT régionaux pour un budget de 17 M€[149] ;
- Bouclier cyber pour les PME : budget de 25 M€[150] ;

[144] Site internet de cybermaveillance.gouv.fr
[145] ANSSI, "Rapport d'activité 2021", mai 2022 et "Rapport d'activité 2022", avril 2023
[146] Cybermalveillance.gouv.fr, "Rapport d'activité 2022", mars 2023
[147] Fevad, communiqué de presse « Baromètre de l'audience du e-commerce : 2ème trimestre 2023 », 27 septembre 2023
[148] Cybermalveillance.gouv.fr, "Rapport d'activité 2022", mars 2023
[149] Observatoire de la Filière de la Confiance Numérique, « Rapport annuel 2023 », juin 2023
[150] Observatoire de la Filière de la Confiance Numérique, « Rapport annuel 2023 », juin 2023

- Budget 2022 de l'ANSSI : 23 M€ (hors masse salariale)[151] ;
- Budget 2022 du GIP ACYMA : 2,7 M€ (dont 0,4 M€ de subvention exceptionnelle de France Relance).

En synthèse, le budget consenti par les acteurs publics/parapublics à la cybersécurité des PME ne représente qu'une goutte d'eau (à titre de comparaison, le budget global alloué à la sécurité routière est de 3,7 Mds€[152]). Alors qu'Emmanuel Moulin, directeur général du Trésor, a affiché ses ambitions de "faire de la Place de Paris un pôle d'expertise en matière d'assurance cyber"[153], le chemin qui reste à parcourir semble long.

Conclusion partielle

L'écosystème au sens large contribue également à expliquer la sous-couverture des PME en assurance cyber.

Des incertitudes juridiques ont freiné et continuent de peser sur le développement du marché de l'assurance cyber, et donc sur son ouverture aux PME.

Dans le domaine de la cybersécurité, le manque de référentiel commun pèse sur les processus de souscription et le déficit de ressources humaines affecte en premier lieu les PME.

Enfin, les acteurs publics et professionnels de la cybersécurité en France sont nombreux et jugés compétents mais cet écosystème est éclaté et doté de moyens financiers limités.

[151] ANSSI, "Rapport d'activité 2022", avril 2023
[152] Ministère de l'intérieur, communiqué de presse "En 2021, comme tous les ans, l'effort financier de l'État en faveur de la sécurité routière (3,7 milliards d'euros par an) est plus de quatre fois supérieur aux recettes des radars automatiques (859 M€ en 2021)", 13 octobre 2022
[153] Direction Générale du Trésor, "Le Développement de l'assurance du risque cyber", septembre 2022

II. Des propositions pour améliorer la protection contre le risque cyber au sein des PME françaises

Dans cette section, nous étudierons différentes mesures pour améliorer la protection des PME contre le risque cyber. Nous nous focaliserons en premier lieu sur le volet de la demande avant de nous concentrer sur les pistes pour "débloquer" le marché de l'assurance-cyber pour les PME françaises. Nous finirons par l'exploration de pistes alternatives.

A. Améliorer la prise de conscience, l'accompagnement, la protection et l'information des PME

1. L'implication des pouvoirs publics dans la sensibilisation et l'accompagnement des PME dans le domaine de la cyber sécurité

Renforcer la prise de conscience des dirigeants de PME face au risque cyber constitue pour nous **le levier prioritaire et urgent** pour initier le cercle vertueux du renforcement de la cyber-résilience du tissu économique national.

Comme le dit Jean-Noël Barrot, Ministre délégué chargé de la transition numérique et des télécommunications[154], « la protection des entreprises contre le risque cyber, y compris en dehors des secteurs d'importance vitale, est plus que jamais un impératif vital sur le plan économique et de la sécurité nationale ». Sur ces bases, une plus grande **implication des pouvoirs publics** nous semble nécessaire.

Notre première recommandation est de **faire de la cybersécurité des PME une grande cause gouvernementale dès 2024** avec deux axes prioritaires : renforcer la prise de conscience et améliorer l'accompagnement des PME.

Dans ce cadre, l'une des premières mesures serait de **créer un organisme qui coordonne les efforts des différents acteurs publics.** Il nous semble important de renforcer l'alignement des (nombreux) acteurs impliqués et de donner davantage de visibilité à leurs actions.

[154] Observatoire de la Filière de la Confiance Numérique, préface du "Rapport annuel 2023", juin 2023

Plusieurs pistes peuvent être explorées : comité interministériel, extension des prérogatives de l'ANSSI (rattachée au Premier Ministre) ou, comme le recommande le CESE[155], organisme rassemblant les différents acteurs impliqués sur le modèle de la Sécurité Routière[156].

Cet organisme bénéficiera naturellement à toutes les parties prenantes, mais nous recommandons qu'une priorité soit accordée, au moins dans un premier temps, aux PME en termes de moyens (humains et financiers).

Dans tous les cas, cet organisme devra être doté d'un fonds interministériel (sur le modèle par exemple du fonds de prévention de la délinquance[157]), afin d'avoir une vision globale du budget alloué (et éviter le morcellement entre les différents acteurs) et des résultats obtenus.

Il nous semble donc urgent de mettre en place un organisme qui coordonne les nombreux efforts des acteurs publics pour gagner en efficacité, au profit notamment des plus vulnérables, dont les PME font partie.

Nous préconisons également le lancement par les pouvoirs publics d'une **campagne massive de communication** qui se voudrait un "**électrochoc**" pour les dirigeants de PME.

Cybermalveillance.gouv.fr a réalisé trois *spots* télévisés en 2022, qui jouent, selon l'organisme, "sur l'humour et le décalage"[158]. Ces *spots* mettent en scène des victimes de cyberattaques : un dirigeant d'une petite entreprise faisant appel à un pigeon voyageur ou bien le maire d'une commune utilisant un "yaourtophone"[159].

Face à l'urgence de la situation, il nous semble nécessaire de changer radicalement de ton pour susciter une prise de conscience rapide des dirigeants de PME.

Nous recommandons ainsi que l'Etat lance rapidement une campagne de communication massive avec des **affiches et des *spots* "chocs"** à l'instar de ce qui a été réalisé par le passé par la Prévention Routière. Cette campagne serait ainsi axée sur les risques encourus par les dirigeants : perturbation durable de l'activité, faillite ou encore engagement de la responsabilité personnelle.

[155] CESE, "Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques", avril 2022
[156] Le Conseil National de la Sécurité Routière a été créé en 2001. Le collège inclut des membres des ministères concernés, des collectivités locales, des associations et des entreprises intéressées par la sécurité routière. https://conseilnational-securiteroutiere.fr/le-cnsr/#le-cnsr-en-bref
[157] Fonds Interministériel de Prévention de la Délinquance créé en 2007 - budget annuel de 2023 de 82 M€ dont 80% reversé aux territoires (www.cipdr.gouv.fr/le-cipdr/le-fipd/)
[158] Cybermalveillance.gouv.fr, "Rapport d'activité 2022", mars 2023
[159] Cybermalveillance.gouv.fr lance la campagne nationale TV-médias « Cybersécurité : de vraies solutions existent » en partenariat avec France Télévisions - Assistance aux victimes de cybermalveillance

Nous estimons le coût d'une telle campagne (affiches et *spots* télévisés pendant deux mois) entre 4 M€ et 5 M€[160].

Toujours dans le cadre de l'action des pouvoirs publics, **un "choc de simplification"** nous semble nécessaire **pour accompagner les PME vers la cybersécurité**.

Selon l'étude de la Fédération Française de la Cybersécurité, le principal frein à la mise en place d'un plan d'action cyber chez les PME est qu'elles ne savent pas "par où commencer" Comme le notent S. Meurant et R. Cardon[161], "la multiplication des outils (...) et des acteurs (...) crée un fort besoin de simplicité et de clarté exprimé par les entrepreneurs".

Nous préconisons la **création d'un "guichet unique"** pour les dirigeants de PME, où ils pourraient trouver l'ensemble des ressources dont ils peuvent avoir besoin (guide d'accompagnement, liste des outils disponibles, formations, possibilité de réaliser un diagnostic de cybersécurité en ligne, possibilité de porter plainte[162] et de demander une assistance en cas de cyber incident,). A ce titre, la plateforme existante cybermalveillance.gouv.fr semble être un candidat naturel pour la poursuite de cet objectif, avec une section dédiée aux PME.

Concernant les contenus disponibles, l'effort peut être considéré comme limité dans la mesure où de nombreuses ressources de qualité (littérature, outils...) existent déjà.

Ce "guichet unique" virtuel gagnerait selon nous à être accompagné d'un **renforcement au niveau régional** en s'appuyant sur les **CSIRT** mis en place par l'ANSSI dans chaque région. L'objectif serait de renforcer leur rôle d'**interlocuteur local de référence**[163] en matière de prévention et de réponse aux incidents cyber. Les objectifs seraient similaires au guichet unique, avec un focus sur la coordination des différents acteurs régionaux.

En complément, les CSIRT pourraient œuvrer, avec les autres acteurs régionaux de référence, à une mise en réseau de responsables de sécurité des systèmes d'information ("RSSI"), comme le

[160] En supposant une diffusion de cinq *spots* par jour sur cinq chaînes nationales pendant huit semaines et un coût moyen de diffusion entre 10 k€ et 15 k€ (le coût dépend des chaines et de l'heure de passage), en complément du coût de réalisation des *spots* (entre 0,5 M€ et 1 M€) et d'une campagne d'affichage massive (entre 0,5 M€ et 1 M€)
[161] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[162] A titre illustratif, il co-existe aujourd'hui quatre sites internet de signalement pour l'hameçonnage, trois plateformes de signalement de délinquance numérique pour la police et la gendarmerie (dont une de plainte en ligne) et une plateforme de pré-plainte en ligne propre au ministère de l'Intérieur
[163] Institut Montaigne, "Cybersécurité : passons à l'échelle", juin 2023

recommandent S. Meurant et R. Cardon[164] ainsi que l'Institut Montaigne[165]. Si l'idée de "partage" de certains RSSI entre plusieurs entreprises semble séduisante, nous avons de sérieux doutes sur sa faisabilité compte tenu de la pénurie de RSSI sur le marché français.

En synthèse, le **renforcement des relais régionaux** nous semble **complémentaire du dispositif internet** afin de sensibiliser un maximum de dirigeants de PME.

Il nous semble par ailleurs prioritaire que les pouvoirs publics lancent rapidement un chantier de **mise en place d'un référentiel commun de cyber sécurité**, qui permettrait de qualifier le niveau de cyber maturité des entreprises.

L'ensemble des acteurs appellent de leurs vœux ce référentiel commun : régulateurs, instituts indépendants, pouvoirs publics, fédérations professionnelles, assureurs et réassureurs.

Nous reprenons ici à notre compte la recommandation de l'Institut Montaigne[166], qui propose la création de ce référentiel avec cinq stades de maturité différents (qui correspondent à cinq "badges", de "graphite" à "platine" pour reprendre leur terminologie[167]). Cette initiative se rapprocherait du référentiel belge de "Cyber Fundamentals"[168] qui comporte quatre niveaux de maturité.

Le niveau socle et plus largement les premiers niveaux du référentiel concerneraient majoritairement les PME, leur permettant de justifier de la mise en place des mesures basiques de sécurité pour se protéger contre les cyberattaques courantes.

Nous proposons que les pouvoirs publics lancent dès que possible un **groupe de travail pluridisciplinaire mené par l'ANSSI,** auquel seraient associés les nombreux acteurs impliqués dans le risque cyber, notamment les assureurs et les réassureurs.

Ces cinq degrés de maturité cyber seraient accompagnés de **cinq niveaux de diagnostic[169]**, dont le résultat fournirait une liste de mesures à adopter pour prétendre à l'atteinte du "badge" visé :

- Pour le badge "graphite" : un diagnostic de premier niveau en ligne, sur la base d'un auto-diagnostic et d'un *scan* externe des systèmes accessibles depuis Internet ;

[164] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[165] Institut Montaigne, "Cybersécurité : passons à l'échelle", juin 2023
[166] Institut Montaigne, "Cybersécurité : passons à l'échelle", juin 2023
[167] Cf. Annexe 3 pour une présentation détaillée du référentiel recommandé par l'Institut Montaigne
[168] Centre for Cyber security Belgium - *https://ccb.belgium.be/en/cyberfundamentals-framework*
[169] Cf. Annexe 3 pour une présentation détaillée des diagnostics recommandés par l'Institut Montaigne

- Pour le badge “bronze” : un diagnostic intermédiaire, de deux heures *in situ*, réalisé par un écosystème de prestataires publics ou privés (reconnus par l’ANSSI) ;
- Pour le badge “argent” : un diagnostic avancé, mené par un écosystème de prestataires certifiés par l’ANSSI : en quatre jours pour un coût estimé à 2 000€ ;
- Pour le badge “ or” : un audit “assurance raisonnable” des systèmes d’information les plus sensibles ou les plus exposés de la structure, par un prestataire qualifié par l’ANSSI ;
- Enfin, pour le badge “platine” : un audit complet des systèmes d’information critiques, qui pourrait être rendu obligatoire pour toutes les entités essentielles[170].

Les PME seraient essentiellement concernées par les trois premiers niveaux d’audit.

Ces diagnostics au coût modéré offriraient une alternative avantageuse aux certifications existantes : à titre illustratif, l’obtention de la norme ISO 27001, reconnue et exigeante, demande un investissement matériel, en termes de temps pour les équipes et en termes de budget (45 k€ pour une PME de 20 salariés d’après le site d’information FeelAgile[171]).

Nous recommandons ainsi la mise en œuvre de cette démarche de mise en place d’un référentiel commun de cybersécurité, incluant les audits associés aux différents stades de maturité cyber. Cette grille permettrait aux dirigeants de PME suffisamment sensibilisés au risque cyber de les guider progressivement vers la cyber sécurité.

En revanche, nous ne sommes pas favorables à rendre obligatoires ces mesures de cybersécurité pour les entreprises. Cette option ne nous parait ni appropriée ni réaliste pour les 4,2M de PME françaises, compte tenu de la complexité du sujet, du manque global de maturité cyber, et du contexte économique actuel.

Nous proposons par ailleurs que les **pouvoirs publics participent directement au financement de cet effort de cybersécurité** visant les PME.

Comme le note un rapport du Sénat de 2021[172], “l’Etat ne peut à la fois enjoindre aux PME de se numériser et ne pas leur donner les moyens financiers d’y procéder en toute sécurité”.

Au-delà des initiatives mentionnées ci-dessus (organisme centralisateur, campagne de communication, guichet unique pour les PME et création d’un référentiel commun de cybersécurité),

[170] Au sens de la Directive NIS 1, puis de la Directive NIS 2
[171] https://feelagile.com/accompagnement-iso-27001/
[172] S. Meurant et R. Cardon, rapport d’information au Sénat fait au nom de la délégation des entreprises “La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?”, juin 2021

nous recommandons que l'Etat prenne les mesures suivantes concernant les diagnostics de cybersécurité :

- **Mise à disposition gratuite d'un outil de *scan* externe**, utilisé pour le diagnostic de premier niveau, sur le site cybermalveillance.gouv.fr ;
- **Financement du second niveau de diagnostic** (2 heures *in situ)* qui serait réalisé par des prestataires reconnus par l'ANSSI ;
- **Octroi d'un crédit d'impôt pour le troisième niveau de diagnostic** (coût unitaire estimé à 2 000€ par l'Institut Montaigne[173] et confirmé par M. Bothorel[174]).

Par ailleurs, nous pensons que l'Etat devrait également **contribuer globalement à l'équipement en cybersécurité via un crédit d'impôt** (ou autre forme d'aide publique) qui couvrirait, au-delà des diagnostics, les dépenses d'équipement et de formation en cybersécurité.

Une option simple serait d'étendre le Crédit Impôt Innovation (de 30%) au domaine de la cybersécurité. Une autre option serait de suivre la recommandation du Sénat en instaurant un crédit d'impôt de 50% dédié à la cybersécurité, avec un montant maximal de 5 000€ par entreprise[175].

Le coût projeté d'une telle mesure, en l'appliquant chaque année à 10 000 PME, se situe dans une fourchette entre 9 M€ et 15 M€ par an.

En complément, l'Etat pourrait **exonérer les PME de la taxe sur les assurances cyber[176]** (9% de la valeur de la cotisation prélevée par l'Etat). Cette mesure serait la plus coûteuse en supposant un doublement ou un triplement du marché de l'assurance cyber des PME chaque année.

Nous préconisons également que les pouvoirs publics financent partiellement l'**effort de formation dans le domaine de la cybersécurité**. Comme évoqué plus haut, le secteur fait face à une pénurie de ressources humaines. Le système français ne forme à l'heure actuelle qu'environ 400 personnes par an alors que les postes à pourvoir se chiffrent à 15 000[177]. Comme évoqué plus haut, ce manque d'experts affecte tout particulièrement les PME.

[173] Institut Montaigne, "Cybersécurité : passons à l'échelle", juillet 2023
[174] Marc Bothorel, Référent national cybersécurité pour la CPME, entretien du 1er juin 2023
[175] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
[176] A titre illustratif, cette taxe fait l'objet d'une exonération pour les véhicules électriques de 2021 à 2023 https://bofip.impots.gouv.fr/bofip/2444-PGP.html/identifiant%3DBOI-TCAS-ASSUR-10-40-50-20210407
[177] Wavestone, communiqué de presse « Maturité cyber en France : une progression notable dans les grandes organisations qui se ressent sur la réussite des cyberattaques », 18 avril 2023

Nous proposons ainsi de **renforcer le dispositif d'apprentissage** accordé aux entreprises engageant des alternants dans le risque cyber. Le montant de l'aide accordée aux employeurs la première année du contrat d'apprentissage, fixé à 6 000 €, passerait à 10 000 €. Des écoles de pointe, comme Guardia à Bordeaux[178], pourraient participer à cet effort. Le coût annuel d'une telle mesure pour 1 000 à 1 500 alternants est estimé entre 4 M€ et 6 M€.

En vision cumulée sur 3 ans, l'effort financier des pouvoirs publics se chiffrerait entre 110 M€ et 215 M€[179]. Hors exonération de la taxe sur les primes d'assurance, le budget global serait ramené dans une fourchette entre 70 M€ et 110 M€.

En supposant que les mesures de financement du diagnostic de niveau 2 et du crédit d'impôt bénéficient essentiellement aux PME hors micro-entreprises, soit une population de 150 000 entreprises, **la mise en œuvre de ce plan d'action sur trois ans pourrait bénéficier à 20% et 30% de la catégorie cible (soit entre 30 000 et 45 000 PME).**

Conclusion partielle

Face à l'urgence de la situation, nous recommandons que le gouvernement fasse de la cybersécurité des PME une de ses grandes causes dès 2024 et mette en place un plan d'action sur trois ans axé autour des principales mesures suivantes :

- La création d'un organisme étatique visant à coordonner les différentes initiatives ;
- Une campagne massive de communication pour créer un "choc" de sensibilisation auprès des dirigeants de PME ;
- La création d'un "guichet unique" pour les PME qui regrouperait l'ensemble des outils et ressources pertinents, accompagnée d'un renforcement des relais régionaux ;
- L'instauration d'un référentiel commun de cybersécurité avec différents niveaux de cyber maturité et de diagnostics associés ;
- La prise en charge partielle de l'État des dépenses de cybersécurité (audit, formation, équipement) et un "coup de pouce" pour les alternants en cybersécurité.

Le coût total de ces mesures sur 3 ans est estimé entre 110 M€ et 215 M€ pour un accompagnement sur la période de 30 000 à 45 000 PME (soit 20% à 30% des PME hors micro-entreprises)

[178] Fondée par des professionnels de la cybersécurité et de l'éducation
[179] Cf. Annexe 4 pour le détail des hypothèses

2. Les mesures pour permettre aux PME d'accéder à des ressources numériques sécurisées

Nous présentons ci-dessous nos recommandations pour rééquilibrer les relations contractuelles entre les acteurs du numérique et les PME et mieux accompagner les dirigeants de PME, souvent à court de moyens, pour évaluer le niveau de cybersécurité de leurs solutions numériques.

En premier lieu, il apparaît nécessaire d'**imposer aux acteurs du numérique de renforcer le niveau de sécurité de leurs produits**.

L'absence d'engagement contractuel n'incite pas aujourd'hui les acteurs du numérique à optimiser le niveau de sécurité de leurs produits. Comme le notent S. Héon et D. Parsoire[180], ces acteurs "créent ainsi une dette de sécurité qui va augmenter au fur et à mesure de la diffusion du produit car il deviendra de plus en plus complexe – et donc cher – de corriger ses failles".

L'entrée en vigueur du ***Cyber Resilience Act***[181], qui vise à **instaurer la "sécurité par défaut", pourrait bousculer cette situation.** Ce règlement[182] porte deux principales ambitions :

- Créer les conditions nécessaires au développement de produits numériques sûrs en limitant les vulnérabilités natives et faire en sorte que les fabricants maintiennent la sécurité dans le temps ;
- Créer les conditions permettant aux utilisateurs de prendre en compte le niveau de cybersécurité lors de la sélection et de l'utilisation de produits numériques.

Néanmoins, l'absence de visibilité sur la date d'entrée en vigueur ou sur les modalités précises d'application soulève plusieurs questions : le texte s'appliquera-t-il seulement aux produits numériques commercialisés après l'entrée en vigueur ou de façon rétroactive ? Quelles seront les modalités concrètes de communication sur le niveau de cybersécurité des produits ? Quel sera l'impact du *lobbying* des acteurs du numérique ?

[180] S. Héon et D. Parsoire, "La Couverture du cyber risque", The Geneva Papers on Risk and Insurance, février 2017
[181] Commission Européenne, "Proposition de règlement du parlement européen et du conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020", 15 septembre 2022
[182] Par définition, ce règlement, une fois approuvé, s'appliquera immédiatement dans tous les états concernés

Ceci nous amène à formuler des **recommandations** qui nous semblent activables **à plus court terme**.

Le Conseil général de l'économie[183] préconise, en plus de la sécurité par défaut, deux mesures concrètes additionnelles :

- **Rendre les mises à jour de sécurité gratuites** (même en l'absence d'abonnement) ;
- **Instaurer l'obligation de fournir des mises à jour de sécurité pendant plusieurs années après la fin de commercialisation** du produit numérique.

Nous recommandons d'explorer ces deux pistes en commençant par une modification de la législation française, puis en intégrant ces mesures dans le *Cyber Resilience Act*.

D'autres pistes existent au **niveau national** pour **rééquilibrer les relations contractuelles entre les acteurs du *cloud* et les PME**.

Nous proposons notamment de **protéger un nombre plus important de PME contre les clause abusives**.

Le Code de la consommation protège en effet les individus et les petites structures (moins de cinq salariés)[184] des **clauses dites abusives**[185]. Nous relayons ici la recommandation du Conseil général de l'économie[186] d'étendre cette protection à davantage d'entreprises, en relevant ce **seuil de 5 à 20 salariés**. Cette réforme pourrait être limitée aux prestataires *cloud* afin d'en faciliter l'adoption.

Cette mesure est soumise à une analyse de faisabilité juridique et pourrait faire l'objet d'actions de *lobbying* des acteurs du *cloud*. Sa capacité de mise en œuvre doit donc être confirmée.

Nous avons choisi ici d'écarter d'autres recommandations du Conseil général de l'économie :

- Modifier la loi pour inclure des obligations accessoires aux contrats *cloud*, notamment un accord sur les niveaux de service (SLA)[187] concernant la disponibilité du service ;
- Instaurer une responsabilité sans faute du fournisseur dans les contrats *cloud* [188].

[183] M. Castellazzi, C. Duchesne-Jeanneney et I. Faucheux, « La Responsabilité des fournisseurs de systèmes numériques », Conseil général de l'économie, de l'industrie, de l'énergie et des technologies, juin 2020
[184] Code de la consommation, article L.221-3. Extension de la protection aux professionnels employant moins de cinq salariés et dont l'objet des contrats n'entre pas dans le champ de l'activité principale du professionnel
[185] Code de la consommation, article L.212-1 "Dans les contrats conclus entre professionnels et consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat"
[186] M. Castellazzi, C. Duchesne-Jeanneney et I. Faucheux, « La Responsabilité des fournisseurs de systèmes numériques », Conseil général de l'économie, de l'industrie, de l'énergie et des technologies, juin 2020
[187] *Service Level Agreement*
[188] Réplication dans le domaine du numérique du régime de responsabilité de fait des produits défectueux

Leur mise en œuvre permettrait un rééquilibrage contractuel mais leur application en France créerait une distorsion de concurrence entre les acteurs français et étrangers et pourrait rendre le marché français moins attractif pour l'innovation. En revanche, il nous semble intéressant de discuter de ces mesures au niveau européen, en travaillant plus globalement sur un "*Small Business Act*" dédié à la cybersécurité des PME, comme le recommande Valéria Faure-Muntian[189].

Au-delà des évolutions du cadre législatif national ou européen, nous prônons la mise en œuvre d'une solution concrète à plus court-terme : le **développement d'une connexion sécurisée au *cloud* « clés en main »[190] pour les plus petites structures,** une mesure prioritaire selon nous**.**

Amazon Web Service (AWS) a mis en place au Royaume-Uni, un dispositif "*Quick Start*"[191] qui configure l'environnement *cloud* en se conformant aux principes du NCSC (l'équivalent britannique de l'ANSSI), avec des mesures d'hygiène informatique comme le nettoyage du trafic.

Lors de son audition dans le cadre des travaux du Sénat[192], le directeur général d'AWS France a mentionné la disponibilité de l'opérateur pour élaborer avec l'ANSSI un dispositif équivalent en France. Nous recommandons la **création dès que possible d'un groupe de travail sous l'égide de l'ANSSI** avec les principaux acteurs du *cloud* **pour une mise en œuvre rapide de ce dispositif de connexion sécurisée au *cloud***.

Conclusion partielle

Plusieurs initiatives sont en cours pour rééquilibrer les relations contractuelles entre PME et acteurs du numérique.

L'ambitieuse Directive NIS2 prévoit d'inclure la "sécurité par défaut" dans les outils et solutions numériques et d'engager la responsabilité des fabricants. Mais le texte est encore en cours de rédaction et le calendrier demeure flou.

D'autres mesures législatives nous semblent pouvoir être mises en œuvre à plus court terme comme la gratuité des mises à jour de sécurité et l'extension de la protection contre les clauses abusives aux PME de moins de 20 salariés.

Enfin, l'instauration rapide d'un groupe de travail entre l'ANSSI et les principaux fournisseurs

[189] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[190] Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018
[191] Résumé du dispositif disponible sur ce site de l'administration britannique. *AWS QUICK START & ASSESSMENT - Digital Marketplace*
[192] S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021

d'accès au *cloud* devrait permettre l'instauration d'un dispositif de connexion sécurisée pour tous.

3. La nécessaire participation de l'écosystème dans cette démarche d'accompagnement des PME

L'ensemble des acteurs liés au risque cyber doivent, selon nous, accompagner les PME françaises dans leur "chemin" vers la cybersécurité.

En premier lieu, les **assureurs** (et les distributeurs d'assurance) ont un rôle clé à jouer pour définitivement **mettre fin à l'ambiguïté liée aux couvertures implicites**. Malgré les efforts déjà réalisés pour clarifier les couvertures dans les polices "traditionnelles", le sujet demeure d'actualité, le dernier communiqué de l'ACPR[193] sur le sujet ayant été publié il y a un an à peine.

Nous appuyons ici la recommandation de l'ACPR[194] et de l'EIOPA[195] qui demandent aux assureurs de mentionner **explicitement** aux entreprises (notamment aux PME) la couverture ou l'exclusion du risque cyber dans leurs polices traditionnelles.

L'EIOPA[196] appelle également de ses vœux un résumé simple et clair dans l'**information précontractuelle** et les **documents publicitaires** des principaux risques couverts et des exclusions, afin de permettre aux clients de prendre une décision éclairée ou de comparer plusieurs polices.

Nous proposons une **accélération du calendrier** sur ce thème, identifié il y a plusieurs années déjà. L'Etat pourrait demander à France Assureurs, à l'APREF et à l'AMRAE notamment de **constituer un groupe de travail** afin d'établir un **plan d'action concret sous six mois avec un calendrier de mise en œuvre rapide**.

En complément, de nombreux acteurs en lien avec les PME ont également selon nous un rôle à jouer pour un meilleur accompagnement des PME dans leur parcours de cybersécurité :

- **Les grandes entreprises**, plus matures en cybersécurité, **pourraient jouer le rôle de *mentors* auprès de leurs fournisseurs et de leurs prestataires de petite taille**, via notamment une mise à disposition de leurs experts en sécurité des systèmes d'information[197].

[193] ACPR. Communiqué de presse "Garanties implicites contenues dans les contrats en matière de couverture du risque cyber", 23 septembre 2022
[194] ACPR. Communiqué de presse "Garanties implicites contenues dans les contrats en matière de couverture du risque cyber", 23 septembre 2022
[195] EIOPA, "Consultation paper on supervisory statement on management of non-affirmative cyber underwriting exposures", mai 2022
[196] EIOPA, "*Consultation paper on supervisory statement on management of non-affirmative cyber underwriting exposures*", mai 2022
[197] Institut Montaigne, "Industrie du futur, prêts, partez !", septembre 2018

Cette recommandation, qui date de 2018[198], nous semble plus que jamais d'actualité à l'approche de l'entrée en vigueur prochaine de NIS2.

Au-delà des aspects liés au *mentoring*, les réglementations qui pèsent sur les grandes entreprises (NIS1, NIS2, DORA) se traduisent par une exigence de *due diligence* approfondie envers les contreparties de taille plus modeste, notamment sur le volet lié à la cybersécurité. Ainsi, dans l'industrie de la défense, les grands acteurs ont déjà développé le programme AirCyber[199] (évaluation de la cyber-maturité, modèles de documentation cyber, outil de détection…) que les PME doivent obligatoirement suivre ;

- **Les métiers du chiffre** (experts comptables et commissaires aux comptes), interlocuteurs de confiance des dirigeants de PME, sont bien positionnés pour participer à l'accompagnement dans le domaine cyber.

  L'Audit Légal de Petites Entreprises[200] prévoit un rapport sur les risques qui inclut le volet cyber[201]. En complément, le CNCC[202] a développé l'application « CyberAudit »[203] d'évaluation du risque cyber et organise de nombreuses formations liées à cet outil.

  L'Institut Montaigne[204] recommande ainsi que les métiers du chiffre réalisent un diagnostic annuel de cybersécurité sur la base d'un cahier des charges construit avec les autorités publiques. Cette piste nous semble intéressante mais nécessite un **effort de formation conséquent auprès des experts comptables et des commissaires aux comptes** avant d'être actionnable. Nous soutenons la mise en œuvre de cette piste à moyen-terme ;

- Les **prestataires informatiques** des PME pourraient davantage jouer le rôle de **prescripteurs de solutions de cybersécurité**, dans une démarche affinitaire, déjà acquise dans de nombreux secteurs. Ils pourraient notamment conseiller des produits d'assurance cyber (avec une rémunération sous forme de **commission**, versée par les courtiers ou les assureurs). A ce titre, les partenariats commerciaux entre prestataires informatiques et assureurs nous semblent une piste prometteuse sur un mode "gagnant/gagnant" ;

[198] Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018
[199] *https://boostaerospace.com/aircyber/* - BoostAeroSpace est le *cloud* privé de l'industrie européenne de l'aérospatiale et de la défense
[200] Audit "allégé" pour les petites entreprises créé par la loi Pacte
[201] En application de la norme d'exercice professionnel 911
[202] Compagnie Nationale des Commissaires aux Comptes
[203] CNCC, https://www.cncc.fr/a-vos-outils/
[204] Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018

- Enfin, les **fédérations professionnelles** et les **chambres consulaires** peuvent également accompagner ces initiatives. La CPME[205] prévoit de livrer en 2024 son propre outil d'analyse de risques cyber, qui a vocation à être très simple[206]. En complément, ces acteurs sont bien placés pour intensifier les efforts de formation auprès des dirigeants et salariés des PME.

La création d'un organisme étatique de centralisation devrait permettre une coordination accrue de ces différents acteurs et ainsi renforcer l'impact de leurs actions.

Conclusion partielle

L'écosystème a également un rôle à jouer pour accompagner les PME dans leur démarche de cybersécurité.
Identifié depuis longtemps, le sujet des garanties silencieuses dans les polices "traditionnelles" doit maintenant être rapidement résolu pour lever toute ambiguïté pour les PME : nous recommandons la création d'un groupe de travail, à l'initiative des pouvoirs publics, qui aurait six mois pour présenter un plan d'actions.
Nous proposons également d'autres pistes de réflexion :

- Faire des grandes entreprises des mentors de cybersécurité pour les PME ;
- S'appuyer sur les réseaux du chiffre (avec un important effort de formation) ;
- Faire des prestataires informatiques des prescripteurs de solutions de cybersécurité ;
- Continuer à s'appuyer sur les fédérations professionnelles et les chambres consulaires.

[205] Marc Bothorel, Référent national cybersécurité pour la CPME, entretien du 1er juin 2023
[206] Quatre profils d'entreprise, 15 questions et des réponses pour aider les dirigeants

B. Faciliter le « déblocage » du marché de l'assurance cyber pour les PME

Dans cette section, nous nous focaliserons sur les mesures qui peuvent se traduire par une augmentation substantielle du taux de couverture en assurance cyber des PME françaises,

Sur la base des données de l'étude LUCY, nous estimons que le marché de l'assurance cyber des PME représente un potentiel de primes de 2,4 Mds€ en 2023[207].

A moyen terme (cinq ans)[208], une pénétration de 40% sur les PME et 10% sur les TPE conduirait à un volume annuel de primes de l'ordre de 615 M€.

A long terme (dix ans)[209], une pénétration de 80% sur les PME et de 25% sur les TPE génèrerait un montant de primes de l'ordre de 2,0 Mds€ par an sur le marché français.

Ce marché offre donc un potentiel attractif pour les assureurs dans les prochaines années.

De nombreuses solutions existent pour accélérer globalement le développement de l'assurance cyber. Nous avons fait le choix d'exclure certaines pistes qui, bien que pertinentes, ne nous semblent pas en mesure d'améliorer significativement la situation des PME dans un horizon de court à moyen terme :

- Clarification du cadre juridique (notamment concernant la cyber guerre) ;
- Amélioration de la lutte contre la cybercriminalité (au niveau national et international).

1. Rendre l'offre d'assurance cyber plus adaptée aux PME

Nous avons évoqué plus haut les difficultés que rencontrent les PME lorsqu'elles initient une démarche de souscription d'une assurance cyber. Afin d'**améliorer l'accès à l'assurance cyber**, nous recommandons la mise en œuvre de **cinq mesures principales** :

- En premier lieu, le **parcours de souscription** doit être **facilité et harmonisé**. La création d'un référentiel commun de cybersécurité (et des différents niveaux de diagnostics) devrait se traduire par une suppression, ou du moins, un **allègement matériel des questionnaires de cybersécurité.**

[207] Hypothèses basées sur l'étude LUCY de l'AMRAE : prime moyenne de 4 000 € pour les 150 000 PME hors micro-entreprises et prime moyenne de 450 € pour les 4,09M de microentreprises
[208] En supposant une inflation des primes de 8% par an
[209] En supposant une inflation des primes de 8% par an

Nous recommandons donc la création d'un **groupe de travail** qui associerait notamment France Assureurs, l'APREF et l'AMRAE pour travailler sur des **propositions concrètes de simplification** de la *due diligence* technique, acceptables par l'ensemble des acteurs de place ;

- Le deuxième angle prioritaire concerne la **clarification** et l'**amélioration de la comparabilité des offres d'assurance cyber**. Nous proposons ici une démarche en deux étapes.

  Dans un premier temps, il nous parait indispensable que les professionnels élaborent ensemble *a minima* une terminologie et des **définitions communes[210]** et **harmonisent la formulation des couvertures et des exclusions**.

  Nous prônons donc, à l'instar de V. Faure-Muntian[211], la mise en place d'un **groupe de travail dédié à cette harmonisation**, en lui donnant six à neuf mois pour restituer ses travaux. Ce groupe pourrait s'organiser sous l'égide de la CSSF[212].

  Dans un second temps, pour aller plus loin, ce même groupe de travail pourrait travailler à la **rédaction de clauses type** pour les PME, voire d'un **contrat-socle** comme le recommandent l'OCDE[213] et V. Faure-Muntian[214]. Ce contrat pourrait inclure des **garanties essentielles** comme l'assistance au redémarrage d'activité, la couverture des pertes d'exploitation et la conformité réglementaire[215]. En s'appuyant sur le **modèle allemand** (qui dispose d'un contrat-socle cyber depuis 2017 comme évoqué plus haut[216]), il pourrait également comporter une série d'**engagements de gestion du risque cyber pris par les entreprises**[217]. Pour que cette démarche soit réellement productive, une déclinaison de ce contrat-socle reflétant les différents profils de risque des PME nous semble nécessaire **;**

[210] ACPR, communiqué de presse "La distribution des garanties contre les risques cyber par les assureurs", 12 novembre 2019 et EIOPA, "*Strategy on cyber underwriting*", février 2020
[211] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[212] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[213] OCDE, "*Unleashing the Potential if the Cyber Insurance Market*", février 2018
[214] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[215] V. Faure-Muntian, Assemblée Générale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
[216] Equivalent de France Assureurs en Allemagne, le *Gesamtverband der Versicherer (GDV)* a notamment créé le programme *Cybersicher https://www.gdv.de/gdv/themen/digitalisierung/initiative-cyber-sicher*
[217] OCDE, "*Unleashing the Potential if the Cyber Insurance Market*", février 2018

- En troisième lieu, **le développement d'une logique d'indemnisation forfaitaire**[218], avec des montants déterminés en fonction des cyber incidents et de leurs conséquences, constitue une piste à explorer.

  C. Arrebolle d'Inquest[219] défend cette position afin de développer le marché de l'assurance cyber des PME, en focalisant la problématique des preneurs de risque sur la fréquence de sinistralité. **Cette piste nous semble prometteuse, au moins à titre temporaire, pour "débloquer" rapidement l'accès à l'assurance cyber pour les PME** ;

- Un quatrième volet pour rendre l'assurance cyber plus accessible aux PME : la **tarification des primes**. Même si le niveau de cybersécurité est partiellement pris en compte dans la tarification, les assureurs pourraient aller plus loin et prévoir des **mécanismes systématiques de réduction de prime** (ou alternativement de réductions de franchises) **liés à l'augmentation du niveau de cybersécurité**. Ils pourraient également encourager la prévention, comme le fait Hiscox[220], avec une **réduction de la franchise si les formations** de son académie cyber **sont suivies** ;

- Cinquième et dernier axe pour améliorer l'accès à l'assurance cyber par les PME : la **création d'offres "packagées" qui intégreraient une couverture assurantielle couplée à un ensemble de services.** Les *insurtech*, à l'image de Dattak, participent à la vulgarisation du risque cyber, tant pour les distributeurs que pour les clients non avertis. La décision récente du premier grossiste français April de référencer les offres de Dattak [221] témoigne que cette combinaison de services et d'assurance répond à un besoin du marché. Toutefois, il nous semble possible d'aller plus loin en élargissant la palette de services et de garanties autour :
  - De la prévention : sauvegardes, gestion de mots de passe, formation ;
  - De l'assurance : souscription simplifiée, indemnisation ;
  - De la gestion de crise : assistance, investigation, gestion de l'attaque.

  Assureurs et sociétés de prestation pourraient nouer des partenariats afin de proposer à leurs clients de telles offres globales, combinant une assurance à une offre de services. La prime

[218] Comme cela peut exister dans certaines polices de garanties d'accidents sur la vie
[219] Christophe Arrebolle, Président d'INQUEST, entretien du 8 mars 2023. Inquest est un acteur de référence dans la gestion des sinistres cyber
[220] Franck Lourdelet, Responsable Partenariats Hiscox France, entretien du 6 juillet 2023
[221] L'Argus de l'Assurance, "Courtage : April s'ouvre à l'assurance cyber", 18 octobre 2023

serait optimisée grâce à la réduction du profil de sinistralité par les mesures de cyber protection.

Conclusion partielle

Les assureurs doivent selon nous contribuer à rendre l'assurance cyber plus accessible aux PME. Nous préconisons cinq mesures :

- Faciliter les parcours de souscription en s'appuyant notamment sur le référentiel commun de cybersécurité ;
- Améliorer la lisibilité et la comparabilité des offres d'assurance cyber :
  - Travail sur une terminologie et des définitions communes dans un premier temps ;
  - Puis, rédaction de clauses type, voire d'un contrat-socle ;
- Engager une réflexion sur une indemnisation forfaitaire, qui pourrait "débloquer" au moins temporairement le marché français ;
- Prévoir des réductions de primes (ou de franchise) automatiques en fonction du niveau de cyber-maturité et de l'effort de formation au risque cyber ;
- Encourager le développement d'offres "packagées" qui offriraient aux PME une réponse globale à leurs besoins : prévention, assurance et assistance.

2. Accélérer le développement du marché de l'assurance cyber pour les PME

Afin d'accélérer le développement du marché de l'assurance cyber pour les PME, nous formulerons dans cette section des pistes qui concernent le secteur de l'assurance et les pouvoirs publics.

Améliorer la connaissance par les assureurs du risque cyber est une priorité afin d'accroître la fiabilité des modèles de risque et de tarification. Parmi les constats unanimement faits par le marché, les données liées au risque cyber des PME sont loin d'être au niveau requis pour alimenter les modèles.

Or, comme le dit le général Aymeric Bonnemaison[222], commandant de la cyberdéfense (Comcyber), face aux particularités de la menace cyber, "le chiffre est le socle de notre protection".

[222] Assemblée nationale, "Compte-rendu - commission de la défense nationale et des forces armées", avril 2023

Nous soutenons donc l'ensemble des pistes de réflexion qui pourraient favoriser **l'enrichissement et le partage d'une base de données des incidents cyber**, notamment :

- La mise en commun anonymisée de tous les incidents connus des acteurs privés (sociétés de gestion des incidents cyber, assureurs...) et publics ;
- La création d'une base de données au niveau européen ou international (sous l'égide de l'ENISA ou de l'OCDE[223] par exemple) ;
- La constitution d'une base de données européenne des sinistres cyber (via la FERMA ?).

Cette amélioration de la connaissance du risque bénéficiera à l'ensemble des parties prenantes mais plus particulièrement aux PME, dont les incidents sont peu déclarés et marginalement assurés.

Bien que ces initiatives nous semblent indispensables à un développement pérenne du marché de l'assurance cyber pour les PME, **elles n'auront pas d'impact tangible avant plusieurs années.**

En complément, face aux spécificités du risque cyber des PME, **le développement de modèles adaptés aux PME apparait également nécessaire**. Les principaux pré requis incluent :

- Une amélioration drastique de la **qualité des données des d'incidents[224]** ;
- L'ajout des informations relatives à l'écosystème de l'entreprise (secteur, etc…) ;
- Le croisement avec **données externes**, permettant notamment aux (ré)assureurs de récupérer un échantillon beaucoup plus large de données[225] ;
- L'utilisation de **techniques d'analyse de données avancées** (apprentissage automatique via *machine learning* et analyses prédictives[226]).

De manière plus spécifique pour les PME, nous recommandons :

- **L'emploi d'approches comme la théorie de la crédibilité[227] ou d'approches bayésiennes[228]**
    - Elles permettent de faire face à la faible taille actuelle des portefeuilles, en ayant recours aux informations disponibles sur une population plus large[229] ;

[223] OCDE, "*Enhancing the Availability of Data for Cyber Insurance Underwriting. The role of public policy and regulation*", février 2020
[224] Descriptif des attaques, pertes financières, coûts de remédiation, etc.
[225] Les assureurs/réassureurs pourraient en contrepartie contribuer à enrichir cette base de données, créant ainsi un cercle vertueux
[226] Approche développée notamment par l'*insurtech* Citalid
[227] Technique actuarielle permettant de mesurer le degré de confiance dans les données sous-jacentes
[228] Approche où la probabilité exprime un degré de croyance dans un événement
[229] O. Lopez et F. Picard, "Cyber-assurance : nouveaux modèles pour quantifier l'impact économique des risques numériques", mars 2019

- **En complément, l'utilisation de modèles épidémiologiques[230]** qui permettent la prise en compte du risque d'accumulation (ou risque systémique).

Nous suggérons que ces propositions soient diffusées largement auprès de la profession par des instances telles que l'Institut des Actuaires, avec des mises à jour régulières.

Pour résumer, améliorer la connaissance du risque cyber nécessite une approche pluridisciplinaire et une collaboration étroite entre les différents acteurs impliqués (publics et privés), dans une approche dynamique qui reflète l'évolution constante des cybermenaces.

L'accélération du développement du marché cyber pour les PME françaises demande également un **renforcement des capacités de distribution**, face au manque d'expertise des courtiers et des agents généraux.

L'axe prioritaire réside selon nous dans la **formation** : nous prônons ainsi l'**intégration obligatoire de modules dédiés au risque cyber dans le cadre de l'obligation de formation annuelle liée à la DDA[231]**.

La Direction du Trésor[232] propose de s'appuyer sur les dispositifs de formation initiale et continue de l'ANSSI, à travers les labels SecNumEdu[233] et SecNumEdu FC[234]. Le dispositif pourrait également mobiliser les grands acteurs de la formation continue en assurance[235].

Une autre option consisterait à étendre significativement les initiatives telles que le partenariat signé en 2021 entre France Assureurs, l'AGEA et la Gendarmerie nationale, pour former et sensibiliser des agents généraux au risque cyber. A ce stade, seuls 800 agents généraux ont été formés dans ce cadre[236], soit 6% de la population visée[237].

Une fois formés, les intermédiaires d'assurance devraient logiquement demander à disposer de produits d'assurance cyber dans leur catalogue. Les conséquences devraient ainsi être :

[230] T. Peyrat, "Risque cyber, un modèle épidémiologique sur réseaux pour le risque d'accumulation du cyber silencieux", mémoire de l'Institut des Actuaires, octobre 2023
[231] Obligation de formation annuelle de 15 heures par an et par collaborateur
[232] Direction Générale du Trésor "Le Développement de l'assurance du risque cyber", septembre 2022
[233] https://secnumacademie.gouv.fr/ : accès aux MOOC de l'ANSSI
[234] Liste des formations continues labellisées SecNumEdu FC disponible sur le site de l'ANSSI : https://www.ssi.gouv.fr/particulier/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/formations-continues-labellisees-secnumedu/
[235] l'IFPASS, l'ESA ou l'ENASS proposent des parcours de formation éligibles à la DDA
[236] Institut Intermédius, *think tank* de Planète CSCA, "Risque cyber : "comment les cabinets de courtage de proximité peuvent-ils s'en prémunir et conseiller leurs clients", septembre 2023
[237] Le nombre d'agents généraux en France est estimé à un peu moins de 13 000, source : www.economie.gouv.fr

- Dans un premier temps, l'intégration d'offres en marque blanche, par le canal du courtage ou de partenariats, comme MAAF Assurances avec Dattak[238] ;
- Ultérieurement, la création d'offres d'assurance par les assureurs français, une fois leurs réseaux matures et les volumes de souscription significatifs.

Cette proposition a été partagée lors de nos échanges avec S. Héon, qui l'a jugée favorablement[239].

Nous préconisons donc le renforcement rapide de la formation des intermédiaires, qui devrait se traduire à terme par un développement de l'offre sur le marché français.

Le levier législatif pourrait également être activé pour accélérer la croissance du marché, en rendant l'**assurance cyber obligatoire**. A ce stade, nous ne recommandons pas cette mesure qui, selon nous, serait mal accueillie par les PME, compte tenu du contexte économique et de leur niveau de maturité en cybersécurité. Cette mesure pourrait en revanche devenir pertinente à moyen terme dans certains secteurs stratégiques et/ou dans le cadre d'appels d'offres publics (en s'inspirant du dispositif "*cyber essentials*" au Royaume-Uni).

Conclusion partielle

Plusieurs pistes nous semblent intéressantes pour accélérer le marché de l'assurance cyber :

- Améliorer la connaissance du risque cyber des PME en encourageant toutes les initiatives permettant un accès à des bases d'incidents enrichies, au niveau national comme international ;
- Améliorer la modélisation du risque cyber des PME en utilisant des méthodes actuarielles alternatives (théorie de la crédibilité, approches bayésiennes, modèles épidémiologiques) ;
    - Ces deux initiatives mettront du temps à porter leurs effets mais elles sont indispensables à un développement pérenne du marché de l'assurance cyber
- Renforcer la formation des distributeurs d'assurance afin qu'ils puissent pleinement jouer leur rôle de prescripteur auprès des dirigeants de PME ;
    - Inclure des modèles cyber obligatoires dans les 15 heures de formation annuelle DDA

En revanche, nous ne préconisons pas à ce stade de rendre l'assurance cyber obligatoire.

[238] Conclu en juin 2023, source interne à MAAF
[239] S. Héon, *Deputy Chief Underwriting Officer – Cyber Solutions*, Scor, entretien du 1er février 2023

3. Étudier des pistes alternatives

Dans cette section, nous envisagerons des pistes alternatives pour renforcer le développement du marché en actionnant soit les leviers de l'offre (avec notamment des pistes qui visent à renforcer les capacités du marché), soit ceux de la demande des PME.

Afin de développer la capacité du marché cyber, qui bénéficierait à toutes les entreprises et particulièrement aux PME, l'**assurance paramétrique** apparait comme une première option.

Il existe aujourd'hui très peu d'offres d'assurance paramétrique dans le domaine du cyber. En France, Descartes Underwriting, spécialisé dans l'assurance paramétrique, étudie à étendre son offre à l'assurance cyber[240]. Aux Etats-Unis, le MGA[241] Intangic propose CyFi[242] une couverture cyber paramétrique, dont le déclenchement est une baisse du cours de bourse supérieure à 15%.

Cette piste mérite d'être explorée[243]. Comme le montrent les études réalisées, la majorité des sinistres cyber des PME est de faible intensité. Le développement d'une offre qui aurait pour critère de déclenchement la durée d'interruption à un service *cloud* par exemple pourrait s'avérer pertinent.

Cette offre présenterait plusieurs avantages : **faible coût**, **souscription et gestion des sinistres simplifiée** (sans recours à des experts) et **délai d'indemnisation très rapide.**

Mais les **freins** sont également **nombreux**.

Du côté des preneurs de risque, la donnée est essentielle à la structuration d'une couverture paramétrique. Or, comme évoqué plus haut, c'est l'un des points faibles du risque cyber. En complément, la forte concentration des prestataires *cloud* crée un risque de cumul important en cas de sinistre pour les preneurs de risque.

Côté demande, cette solution ne couvrirait qu'une partie des risque : elle n'intègre ni le volet responsabilité civile, ni le volet assistance, et n'est pas adaptée aux sinistres majeurs[244].

Notre opinion est que cette alternative mérite d'être explorée mais qu'elle a **davantage le profil d'un complément de couverture** plutôt que le caractère d'une solution concrète pour les PME.

[240] Les Echos, "*Insurtech* : la data au service du *risk management*", 1er février 2023
[241] *Managing General Agent*
[242] Insurer Intelligent, *"Parametric cyber: turning the market on its head"*, 27 mars 2023
[243] Direction Générale du Trésor "Le Développement de l'assurance du risque cyber", septembre 2022
[244] Institut des Actuaires, "Note sur l'assurance paramétrique : cas particulier du risque cyber", 2021

Une autre option pour limiter les freins de capacité du marché cyber consisterait à envisager la **création d'un *pool* d'assureurs avec la participation de l'État**.

La récente attaque par rançongiciel de MoveIT (logiciel de partage de données) en mai dernier, qui aurait impacté plus de 2 500 organisations et 60 millions de particuliers[245] nous rappelle le caractère systémique du risque cyber, scénario auquel les PME seraient particulièrement exposées. Or, le secteur de l'assurance ne peut pas à lui seul faire face à ce type d'événement,[246] dont les conséquences financières pour la France seulement se chiffreraient en milliards d'euros[247].

Dans ce contexte, de nombreux acteurs (OCDE[248], chercheurs[249], acteurs du risque et de l'assurance[250]) appellent à la création d'un *pool* rassemblant assureurs et réassureurs avec le concours de l'Etat, ou, plus largement, au niveau européen. Ce *pool* pourrait s'inspirer des mécanismes existants en France et en Europe dédiés à des risques comme le terrorisme ou les catastrophes naturelles.

Les bénéfices attendus seraient nombreux : capacité accrue, meilleure connaissance du risque, diversification renforcée et couvertures harmonisées[251].

En France, les dernières discussions avec les pouvoirs publics concernant l'instauration d'un tel mécanisme remontent au **projet CATEX**[252] pendant la pandémie du Covid-19 en 2020.

Ce projet visait à mettre en place un système de partage de risque entre entreprises, assureurs, réassureurs et pouvoirs publics. L'objectif, dans sa version de novembre 2020, était de couvrir les entreprises contre les conséquences financières d'une fermeture administrative en cas de pandémie/épidémie, en versant un "capital résilience". Dans la version présentée plus tôt aux pouvoirs publics en juin 2020, la profession proposait déjà un champ d'application plus large de la couverture à tous les risques systémiques, en incluant notamment le risque cyber.

[245] Emisoft, "*Unpacking the MOVEit Breach: Statistics and Analysis*", données au 26 octobre 2023
[246] RA. Carter, D. Pain et J. Enoizi, "*Insuring Hostile Cyber Activity: in search of sustainable solutions*", The Geneva Association, janvier 2022
[247] Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018
[248] OCDE, "*Enhancing the Role of Insurance Cyber Risk Management*", novembre 2017
[249] RA. Carter, D. Pain et J. Enoizi, "*Insuring Hostile Cyber Activity: in search of sustainable solutions*", The Geneva Association, janvier 2022, M. Eling et JH. Wirfs, "*Cyber Risk: Too Big To Insure*", University of St Gallen et Swiss Re, 2016 et M. Eling et W. Schnell, "*Ten Key Questions on Cyber Risk & Cyber Risk Insurance*", The Geneva Association, novembre 2016
[250] Allianz, Axa HDI, Howden, Marsh, Lloyds, MunichRe, FERMA, "*How Can Europe Lead the Way to Cyber Resilience*", juin 2023
[251] M. Eling et JH. Wirfs, "*Cyber Risk: Too Big To Insure*", University of St Gallen et Swiss Re, 2016
[252] Cf. Annexe 5 et présentation du projet CATEX sur le site de France Assureurs en date du 26 novembre 2020 : https://www.franceassureurs.fr/nos-positions/lassurance-qui-protege/projet-catex/

Le rejet de la proposition par l'Etat, dans un contexte de réduction de la dette et de dégradation du pouvoir d'achat, illustre la position des pouvoirs publics à date :

- Ne pas exposer les comptes publics à une volatilité accrue liée à des risques croissants, majeurs et incertains. La situation de la CCR dans le cadre du régime des Cat Nat expose déjà largement l'Etat, dont le risque de devoir activer sa garantie (si les sinistres atteignent 90% les réserves de la CCR) se rapproche sensiblement[253] ;
- Préserver le pouvoir d'achat des citoyens et la situation financière des PME qui supportent déjà des charges lourdes et inflationnistes.

Bien que les orientations à court terme des pouvoirs publics excluent un tel système de *pool*, **nous préconisons que la profession ouvre à nouveau les réflexions pour élaborer un montage de ce type**, peut-être en éloignant le niveau de l'intervention de l'Etat et en limitant le dispositif dans le temps. Une alternative serait de lancer une initiative au niveau européen.

Comme le mentionne Michael Powers[254], l'Etat, à l'inverse des assureurs, ne peut éviter aucune catégorie de risque. Il doit donc accepter toutes les expositions conduisant à une sinistralité très élevée (et ce quelle que soit la fréquence). Mais, la constitution de réserves pour couvrir ces risques majeurs constitue souvent une décision politique difficile à prendre, les gouvernements ayant ainsi tendance à attendre que le sinistre se produise pour réagir. **Nous encourageons donc les acteurs publics à participer aux réflexions sur la création d'un tel *pool***. Une inaction pourrait en effet exposer les comptes publics de manière bien plus importante au titre de la solidarité nationale si une attaque majeure venait à faire tomber une large partie des PME qui constituent le cœur du tissu économique français.

En contrepartie de son refus du projet CATEX, le gouvernement a notamment ouvert la possibilité à une révision des règles de calcul de la **provision d'égalisation[255]** pour les sociétés d'assurance, afin d'**élargir son champ d'application** notamment au **risque cyber.**

Cette piste, que nous soutenons, améliorerait la résilience des sociétés d'assurance les années de sur-sinistralité, en leur permettant d'utiliser les réserves constituées les années de faible sinistralité. Cette

[253] S. Marsaud et S. Rousseau, Assemblée Nationale, Comité d'évaluation et de contrôle des politiques publiques, "Rapport sur l'évaluation de la prise en compte du retrait-gonflement des argiles", mars 2023
[254] Michael Powers, "*Acts of God and Man*", Columbia Business School Publishing, 2012
[255] Article R331-36 du Code des assurance : provision destinée à faire face aux charges exceptionnelles afférentes aux opérations garantissant les risques dus à des éléments naturels, le risque atomique, les risques de responsabilité civile dus à la pollution, les risques spatiaux, les risques liés au transport aérien, et les risques liés aux attentats et au terrorisme, et calculée dans les conditions fixées par la loi.

mesure permettrait ainsi aux assureurs de continuer à déployer des capacités pour accompagner le marché pendant sa montée en maturité en limitant la volatilité sur ces portefeuilles de contrats.

Les derniers développements sur le sujet ne laissent guère présager d'un élargissement de la Provision d'Égalisation en normes comptables françaises à court terme. Le recours aux captives luxembourgeoises (actuellement majoritaires) reste donc un levier à disposition des assureurs.

Autre levier identifié pour augmenter la capacité du marché cyber : **le recours aux marchés financiers avec l'émission d'*Insurance-linked Securities* ou de *cyber bonds***.

A l'instar de l'émission de Beazley[256] ou encore plus récemment d'AXIS[257], les marchés financiers démontrent une possibilité d'accès à du capital complémentaire pour les assureurs/réassureurs.

L'accès aux marchés financiers se concentre aujourd'hui sur des périmètres bien définis et relativement maîtrisés, ce qui, comme nous l'avons démontré, n'est pas le cas du segment des PME.

Cette option ne pourra donc être envisagée pour les PME qu'une fois que le marché primaire de l'assurance cyber sur ce segment sera mieux maîtrisé.

Notre dernière piste concerne le développement de l'auto-assurance des PME, via la création de **captives associant plusieurs entreprises**.

La loi de Finances 2023 a entériné la création d'un régime dédié aux captives de réassurance en France pour les sociétés non financières. Mais, **ces mécanismes semblent loin d'être à la portée des PME**.

La captive appartient par définition à une seule société, il semble donc compliqué, mais pas impossible, de créer des véhicules communs à plusieurs PME[258], peut-être par secteur d'activité ou par région, mais la mise en œuvre demeure complexe.

Une piste pourrait être envisagée : les **captives situées à Malte,** généralement détenues et gérées par les courtiers, ont la particularité de proposer de louer des **compartiments** (indépendants entre eux). Cette approche devrait à minima **réduire le coût** d'accès à la captive pour les PME (à voir dans quelle mesure il serait supportable). Aussi, la localisation géographique et la langue peuvent constituer des freins pour de nombreuses PME.

[256] Beazley, communiqué de presse "*Beazley launches market's first cyber catastrophe bond*", 9 janvier 2023
[257] Business Insurance, "*Axis Capital sponsors $75 million cyber cat bond*", 19 octobre 2023
[258] Direction Générale du Trésor "Le Développement de l'assurance du risque cyber", septembre 2022

Théoriquement, ce système semble vertueux mais n'est malheureusement que peu voire pas accessible à la plupart des PME. En effet, la mise en place d'une captive de réassurance nécessite d'avoir des connaissances poussées en assurance (les captives sont soumises à la réglementation Solvabilité II), de mobiliser des capitaux pour couvrir les risques et de mettre en place des équipes dédiées.

Conclusion partielle

Le marché de l'assurance cyber fait face à des problèmes de capacité qu'il nous semble intéressant d'adresser pour permettre le développement de la couverture assurantielle des PME.
Nous avons exploré plusieurs pistes qui présentent toutes des limites ou des complexités de mise en œuvre :

- L'assurance paramétrique : approche intellectuellement intéressante mais qui se heurte au manque de données disponibles et qui ne couvre que partiellement le risque ;
- La création d'un *pool* d'assureurs avec l'Etat ou au niveau européen : malgré sa difficulté de mise en œuvre (comme l'illustre le récent échec du projet CATEX), cette piste doit être poursuivie pour permettre un développement pérenne de l'assurance cyber ;
- La révision des règles de provision d'égalisation afin de l'étendre au risque cyber : cette piste que nous recommandons se heurte à ce stade à un blocage des pouvoirs publics ;
- Le recours aux marchés financiers via l'émission de *cyber bonds* : une piste prometteuse à terme mais dont le potentiel à court terme demeure limité vu le manque de données ;
- La création de captives associant plusieurs PME : solution intellectuellement intéressante mais complexe et coûteuse à mettre en œuvre.

Ainsi, aucune solution ne se dégage nettement à date, mais nous encourageons les différents acteurs privés et publics à poursuivre les réflexions sur ces sujets, afin d'augmenter les capacités futures du marché de l'assurance cyber.

Conclusion

Le sujet de la cybersécurité des entreprises françaises, et plus particulièrement des PME, a donné lieu ces dernières années à de nombreuses études et publications, assorties de multiples recommandations. Dans le même temps, les initiatives des acteurs publics et privés se sont développées afin de sensibiliser et d'accompagner les PME françaises dans leur démarche de cybersécurité. Seuls les assureurs français sont finalement restés en retrait de ce sujet, à date.

Malgré les progrès réalisés ces dernières années, nous sommes persuadés de la nécessité d'accélérer le tempo de façon significative face à une cybermenace de plus en plus sophistiquée.

Notre conviction majeure est que la **priorité** porte sur le volet de la demande en **sensibilisant massivement les dirigeants de PME** sur les risques encourus ; et qu'une fois sensibilisés, la priorité est de **les accompagner progressivement dans leur démarche de cybersécurité**.

L'Etat a, selon nous, un rôle clé à jouer, afin d'impulser cette accélération. Nous proposons donc que le **gouvernement** fasse de la **cybersécurité des PME une de ses causes prioritaires dès 2024**. Dans ce cadre, un plan à trois ans serait mis en œuvre avec la création d'un organe de centralisation (indispensable pour coordonner les différentes initiatives), une campagne de communication "choc" visant les dirigeants de PME et un guichet unique d'entrée pour les PME avec l'ensemble des ressources dont elles ont besoin. Nous recommandons également la mise en place rapide d'un référentiel commun de cybersécurité, prévoyant différents niveaux de cyber-maturité afin de pouvoir correspondre à toutes les entreprises ainsi qu'une contribution financière à ces efforts de cybersécurité

Nous avons chiffré l'effort financier des pouvoirs publics sur trois ans entre 110 M€ et 215 M€, ce qui nous semble être un effort raisonnable en rapport des enjeux stratégiques.

Les professionnels de l'assurance ont également un rôle à jouer pour mieux informer les entreprises sur leurs couvertures actuelles, travailler à une offre d'assurance cyber clarifiée et harmonisée avec des parcours de souscription simplifiés. Dans ce contexte, nous pensons que le **développement d'offres globales à destination des PME intégrant prévention, équipement en cybersécurité, assurance et assistance** en cas d'incident, présente d'intéressantes perspectives.

Nous recommandons également d'intensifier significativement la formation des courtiers et agents généraux dans la connaissance du risque cyber et des solutions d'assurance, afin qu'ils jouent pleinement leur rôle de courroie de transmission auprès des dirigeants de PME.

Enfin, le marché de **l'assurance cyber souffre globalement de capacités insuffisantes**. Bien que ce problème ne vise pas spécifiquement les PME, un développement pérenne de l'assurance cyber pour les PME ne peut être envisagé sans une augmentation des capacités globales. Nous évoquons plusieurs pistes dans ce mémoire, toutes sont complexes à mettre en œuvre et demandent que la profession, les acteurs publics et le monde universitaire continuent la réflexion et les travaux sur ce thème. La création d'un *pool* d'assureurs, avec le concours de l'Etat, nous semble être la piste prioritaire à explorer.

Un autre moyen de mieux couvrir les PME françaises contre le risque cyber serait le développement d'offres dédiées par les principaux acteurs français. Axa est en effet aujourd'hui le seul assureur national avec une présence significative sur ce segment. Bien que le risque cyber soir complexe pour les preneurs de risque, nous appelons de nos vœux un **développement de l'offre par les autres grands acteurs français**. Nous pensons que la mobilisation des intermédiaires, via notamment la contrainte de formation, pourrait inciter leurs mandantes à développer des offres dédiées au cyber avant que le marché ne prenne son essor.

En conclusion, le choix du thème de ce mémoire peut interpeller dans la mesure où aucun membre de ce groupe de travail n'avait de connaissance particulière dans le domaine du risque cyber. Ce thème de la cybersécurité nous a réunis car nous partagions la volonté de rédiger un **mémoire utile**, qui recommanderait des **propositions concrètes et actionnables dans un horizon de temps court**. Nous espérons ainsi apporter notre contribution à l'ensemble des réflexions qui portent sur ce thème stratégique de la cybersécurité de nos PME.

Annexes

Annexe 1 - Synthèse des résultats de l'étude LUCY de l'AMRAE

Depuis 2021, l'AMRAE publie chaque son étude LUCY (LUmière sur la CYberassurance).

Bien que non exhaustive (notamment sur le segment des plus petites entreprises), cette étude constitue la meilleure source de données sur le marché de l'assurance-cyber en France.

L'étude est réalisée en partenariat avec des courtiers : AON, Diot-Siaci, Filhet Allard, Marsh, Verlingue, Verspieren, WTW, SMABTP (depuis l'édition 2022), Dattak et Howden (ces deux derniers depuis l'édition 2023). Aux courtiers s'ajoute Planète CSCA, le syndicat des courtiers d'assurance afin d'avoir une meilleure vision des PME.

Les définitions utilisées par l'étude sont les suivantes

- Grandes entreprises : chiffre d'affaires supérieur à 1,5 Md€ ;
- Entreprises de taille intermédiaire (ETI) : chiffre d'affaires entre 50 M€ et 1,5 Md€ ;
- Entreprises de taille moyenne : chiffre d'affaires entre 10 M€ et 50 M€ ;
- Petites entreprises : chiffre d'affaires entre 2 M€ et 10 M€ ;
- Micro-entreprises (TPE) : moins de 2 M€ de chiffre d'affaires.

L'étude se focalise sur les trois premiers segments décrits ci-dessus.

Le tableau ci-dessous synthétise les principales données chiffrées de l'enquête.

	2019	2020	2021	2022
Périmètre étude				
Nombre d'entreprises	1 879	1 879	2 028	9 672
Nombre de sinistres indemnisés			518	177
Primes (MEUR)	**87**	**130**	**185**	**316**
- *croissance*		*49%*	*42%*	*71%*
Sinistres (MEUR)	**73**	**217**	**164**	**71**
- *croissance*		*197%*	*-24%*	*-57%*
Ratio S/P	**84%**	**167%**	**88%**	**22%**
Ratio S/P par catégories				
- Grandes Entreprises	44%	190%	58%	16%
- ETI	481%	85%	261%	51%
- Moyennes entreprises	Nd	45%	36%	100%
Taux de couverture				
- Grandes Entreprises	72%	87%	84%	94%
- ETI	Nd	8%	9%	10%
- Moyennes entreprises	Nd	0,003%	0,20%	3%
Taux de primes				
- Grandes Entreprises	0,93%	1,02%	2,02%	2,70%
- ETI	0,32%	0,45%	0,70%	1,07%
- Moyennes entreprises	0,49%	0,71%	0,32%	0,40%

Annexe 2 - Critères d'assurabilité de Berliner

Baruch Berliner a publié en 1982 un ouvrage intitulé "Limits of Insurability of Risks". Son analyse identifie 9 critères principaux d'assurabilité, regroupés en trois catégories et décrits dans le tableau ci-dessous. Cette synthèse est basée sur les travaux de C. Biener, M. Eling et JH. Wirfs, *"Insurabillity of Cyber Risk"*, The Geneva Association, août 2014.

	Catégorie	Critère	Caractéristique
1	**Actuariat**	Occurrence des sinistres	Indépendante
2		Perte maximale potentielle	Soutenable
3		Perte moyenne par sinistre	Modérée
4		Exposition aux pertes	Fréquence minimale de sinistralité
5		Aléa moral et antisélection	Non excessif
6	**Marché**	Primes	Couverture des coûts pour les assureurs et niveau acceptable pour les souscripteurs
7		Limites de couverture	Acceptables
8	**Société**	Politique publique	Cohérence avec les valeurs sociétales
9		Restrictions légales	Autorisent la couverture

Annexe 3 - Les cinq niveaux de maturité cyber proposés par l'Institut Montaigne

Source : Institut Montaigne, « Cybersécurité : passons à l'échelle », juin 2023

Critères / Badges	Graphite	Bronze	Argent	Or	Platine (OIV/OSE)
Qui suis-je (entité type)	TPE (PME < 10 salariés) Très petite collectivité (-1000 hab) ~ 1 000 000	PME entre 10 et 50 salariés Petite collectivité (1000 à 5000 hab, syndicats mixtes) ~ 150 000	ETI et PME > 50 (hors NIS 2) Moyenne collectivité (+5000 hab, EPCI) ~ 35 000	"Entités importantes" NIS 2 Grande collectivité ~ 10 000	OIV + OSE NIS ("entités essentielles" NIS 2) ~ 700
Je connais mes vulnérabilités (diagnostic / audit)	Autoévaluation En ligne avec scan externe	In situ 2h Gratuit, ou prestataire labellisé	In situ 4 jours Prestataire certifié (2000€)	Audit PASSI RGS	Audit PASSI LPM
Je me forme et m'entoure (compétences numériques de gouvernance)	Sensibilisation dirigeant 2h ACYMA	Conseiller (CSN) + MOOC SecNum académie	MOOC + CSN + RSSI temps partagé	MOOC + CSN + RSSI temps plein	N/A
J'acculture mon équipe (procédure de gestion d'attaque)	Alerte "incendie" cyber	Exercice de simulation d'attaque simple	Exercice avancé (PCA/PRA partiel)	Exercice de crise (PCA/PRA complet)	Homologuée
J'anticipe l'interruption d'activité (provision pour risque cyber / garanties offertes par la police d'assurance)	Préparation et diffusion d'une liste de bonnes pratiques à la suite de l'alerte incendie cyber	Provision pour risque cyber (2 % du chiffre d'affaires annuel)	Assurance gestion de crise (versements rapides forfaitaires)	Assurance gestion de crise + RC cyber de l'entreprise et du dirigeant	Obligations spécifiques OIV/OSE
Je fais appel à des professionnels formés/vérifiés	Tout professionnel	Labellisés Expert Cyber[151]	Certifiés ANSSI	Qualifiés ANSSI	

Critères Badges	Graphite	Bronze	Argent	Or	Platine (OIV/OSE)
J'organise mes sauvegardes et mes données	+	+	++	++	
Je protège les points d'entrée de mon SI	+	+	++	+++	
Je sécurise mes données et applications	+	+	++	+++	
Je protège les postes de mon SI	+	++	+++	++++	
Je sécurise le réseau de mon SI	+	++	+++	+++++	
Je centralise et supervise mon SI pour mieux détecter et traiter les menaces	+	++	+++	+++++++	
Quelle durée de validité	1 an	2 ans	2 ans	3 ans	3 ans

Annexe 4 - Chiffrage indicatif du coût des mesures financées par les pouvoirs publics

Le tableau ci-dessous présente le détail des hypothèses retenues pour le calcul du coût des mesures de financement par les pouvoirs publics que nous recommandons dans ce mémoire.

Coûts des mesures pour les pouvoirs publics (MEUR	Année 1		Année 2		Année 3	
Mesure	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**
Organisme de centralisation	1,0	2,0	1,0	2,0	1,0	2,0
Campagne de communication	4,0	5,0	4,0	5,0	4,0	5,0
Guichet unique PME sur cybermalveillance	1,0	1,5	0,2	0,3	0,2	0,3
Numéro d'appel 24/24 7/7	0,5	0,8	0,5	0,8	0,5	0,8
Budget groupe de travail ANSSI (référentiel)	0,3	0,5	-	-	-	-
Outil de scan externe	0,1	0,2	0,1	0,2	0,1	0,2
Financement diagnostic de niveau 2	4,0	6,0	4,0	6,0	4,0	6,0
Crédit impôt	9,0	15,0	9,0	15,0	9,0	15,0
Exonération taxe sur primes assurance cyber	5,4	8,1	10,8	24,3	21,6	72,9
Alternants cybersécurité	4,0	6,0	4,0	6,0	4,0	6,0
Total	**29,3**	**45,1**	**33,6**	**59,6**	**44,4**	**108,2**

Cumul 3 ans	**107,4**	**212,9**

Les principales hypothèses sont les suivantes

- Effort financier sur trois ans ;
- Organisme de centralisation : hypothèse du budget annuel de fonctionnement ;
- Campagne de communication :
    - Diffusion de cinq *spots* par jour sur cinq chaînes nationales pendant huit semaines en supposant un coût moyen de diffusion entre 10 k€ et 15 k€ (le coût dépend des chaines et de l'heure de passage) ;
    - Coût de réalisation des *spots* (entre 0,5 M€ et 1 M€) ;
    - Campagne d'affichage massive (entre 0,5 M€ et 1 M€) ;
- Guichet unique pour les PME sur le site cybermalveillance.gouv.fr :
    - Le chiffrage de la première année reflète le coût de construction sur le site de la section dédiée aux PME ;
    - L'estimation des années suivantes reflète le coût annuel de maintenance et de mise à jour ;
- Numéro d'appel d'urgence :
    - 3 k€ par ETP et par mois, entre 10 et 15 ETP ;
    - Application d'un multiple de 1,5x pour refléter les frais de structure ;

- Groupe de travail sous l'égide de l'ANSSI pour l'adoption d'un référentiel commun de cybersécurité : entre 0,3 M€ et 0,5 M€ (en année 1 seulement) ;
- Outil de *scan* externe : coût de mise à disposition sur le site cybermaveillance.gouv.fr estimé entre 0,1 M€ et 0,2 M€ par an ;
- Financement du diagnostic de niveau 2 (2h *in situ*) :
    - Hypothèse de 10 000 à 15 000 audits par an pour un coût unitaire de 400 € ;
- Crédit d'impôt sur les dépenses liées à la cybersécurité (équipement, diagnostic poussé, formation, ...) :
    - Borne basse : crédit d'impôt de 30% bénéficiant à 10 000 entreprises par an pour un montant moyen de dépenses de 3 000 € ;
    - Borne haute : crédit d'impôt de 50% sur la base des mêmes hypothèses.
- Exonération de la taxe sur les primes d'assurance cyber pour les PME :
    - Montant des primes d'assurance cyber des PME en 2022 : 9,5 M€ en 2022 selon l'étude LUCY[259] ;
    - Hypothèse de croissance annuelle du marché de 200% à 300% par an (en supposant que l'année 1 est 2024) ;
    - Hypothèse de maintien du taux de taxe sur les primes d'assurance à 9% ;
- Alternants en cybersécurité :
    - Hypothèse d'une aide supplémentaire de 4 000 € par alternant ;
    - Nombre d'alternants concernés : entre 1 000 et 1 500 par an.

[259] Cf. Annexe 1

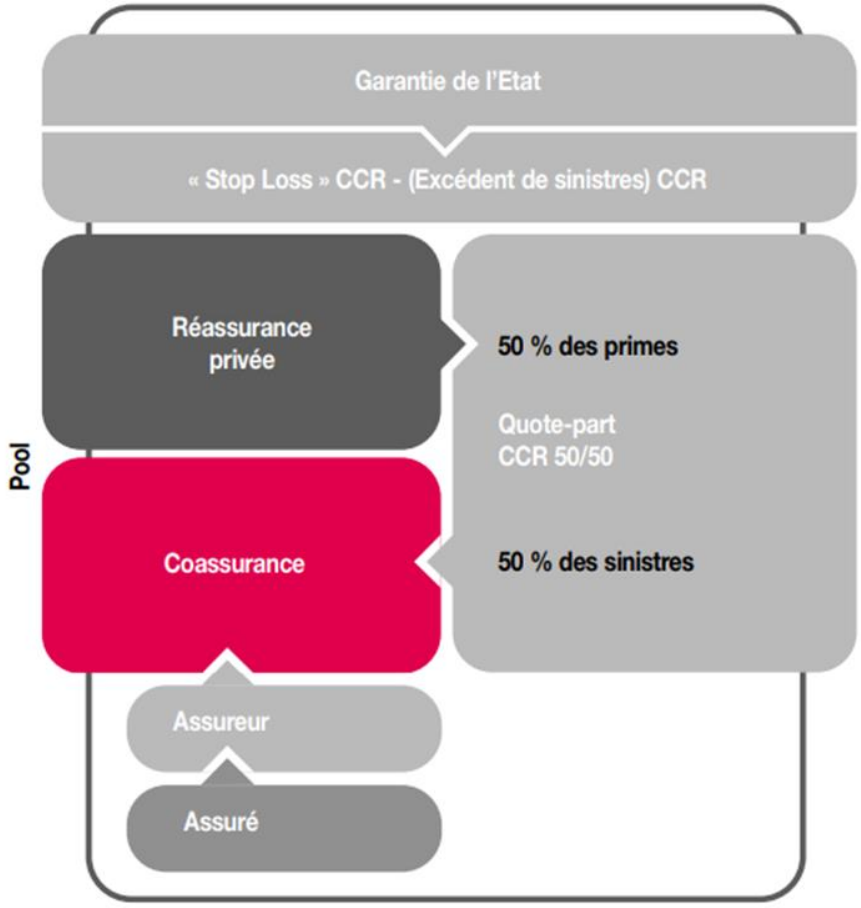
Annexe 5 - Illustration du projet CATEX

Le projet CATEX a été lancé à l'initiative de France Assureurs au début de la pandémie de Covid-19 (via un groupe de travail associant assureurs et réassureurs). La version définitive du projet a été rendue publique en novembre 2020.

L'objectif de ce projet est de couvrir les entreprises contre les impacts économiques d'une fermeture des établissements décidée par les pouvoirs publics, en leur versant un "capital résilience".

Le champ d'application concerne l'ensemble des entreprises disposant d'un contrat d'assurance multirisque.

Le schéma ci-dessous illustre le fonctionnement du dispositif.



Source : France Assureurs, 2020.

Annexe 6 - Synthèse des recommandations du mémoire

Le tableau ci-dessous synthétise les recommandations de notre mémoire. Nous y avons ajouté un niveau de priorité (P1/P2/P3) et un horizon de temps de mise en œuvre (court-terme, moyen-terme, long-terme).

	Recommandation	Priorité	Horizon
1	**Faire de la cybersécurité des PME une grande cause gouvernementale dès 2024 avec un plan d'action à 3 ans**		
	- Créer un organisme de coordination	P1	CT
	- Lancer une campagne massive de communication « choc »	P1	CT
	- Créer un guichet unique pour les PME sur le site cybermalveillnce.gouv.fr	P1	CT
	- Renforcement des relais régionaux en s'appuyant sur les CSIRT de l'ANSSI	P2	CT
	- Constituer un groupe de travail pluridisciplinaire sous l'égide de l'ANSSI pour la mise en place d'un référentiel commun de cybersécurité	P1	CT
	- Mettre à disposition des PME gratuitement un outil de *scan* externe (diagnostic de niveau 1)	P1	CT
	- Financer un diagnostic de niveau 2 (2h *in situ*) pour les PME	P2	CT
	- Octroyer un crédit d'impôt (entre 30% et 50%) sur les dépenses de cybersécurité (équipement, audit poussé, formations)	P1	CT
	- Bonifier la subvention des alternants en cybersécurité (de 6k€ à 10k€)	P2	CT
2	**Imposer aux acteurs du numérique de renforcer le niveau de sécurité de leurs produits**		
	- Encourager la mise en œuvre de la Directive NIS2 sur ces aspects	P2	CT/MT
	- Modifier la loi française (et étendre à NIS2) pour inclure deux obligations : gratuité des mises à jour de sécurité et disponibilité de ces mises à jour [x] années après la fin de commercialisation	P2	CT/MT
	- Etendre la protection contre les « clauses abusives » aux PME de moins de 20 salariés	P2	CT/MT
	- Envisager de lancer au niveau européen un *Small Business Act* dédié à la cybersécurité des PME	P2	CT/MT
	- Mettre en œuvre rapidement un dispositif de connexion sécurisée au *cloud* pour les PME	P1	CT
3	**Enjoindre l'écosystème à accompagner le développement de la cybersécurité des PME**		
	- Assureurs : mettre fin à l'ambiguïté des « garanties silencieuses » - via groupe de travail pour remise d'un plan d'action sous 6 mois	P1	CT
	- Grandes entreprises : les encourager (via les fédérations professionnelles) à jouer le rôle de mentor des PME	P2	CT/MT
	- Métiers du chiffre : réalisation d'un diagnostic annuel de cybersécurité	P3	MT/LT
	- Prestataires informatiques : développement du rôle de prescripteurs de solutions de cybersécurité et d'assurance cyber	P2	CT/MT
	- Agences de notation ou d'information sur les entreprises (Coface, Ellisphère) : prise en compte des aspects cyber dans leur notation	P3	MT
	- Fédérations professionnelles et chambres consulaires : en appui des initiatives locales – rôle dans le développement de la formation	P2	CT/MT

	Recommandation	Priorité	Horizon
4	**Rendre l'assurance cyber plus adaptée aux PME**		
	- Faciliter le parcours de souscription via l'allègement de la *due diligence* technique	P1	CT
	- Harmoniser les définitions, la terminologie, les couvertures et les exclusions des polices d'assurance cyber (groupe de travail sous l'égide de la CSSF)	P1	CT
	- Approfondir cette harmonisation en rédigeant des clauses type ou un contrat-socle pour les PME (sur le modèle allemand)	P2	CT/MT
	- Initier une réflexion sur le développement d'une indemnisation forfaitaire des risques cyber qui pourrait être une mesure transitoire	P2	CT/MT
	- Proposer dans les polices d'assurance cyber une réduction des primes (ou des franchises) liées à l'augmentation du niveau de cybersécurité ou le suivi de formation sur le risque cyber	P2	CT/MT
	- Créer des offres « packagées » à destination des PME incluant prévention, assurance et assistance en cas de cyber incident	P2	CT/MT
5	**Accélérer le développement du marché de l'assurance cyber**		
	- Encourager toutes les initiatives permettant d'enrichir les bases d'incident cyber au niveau national, européen et international	P2	MT/LT
	- Encourager la profession de l'assurance, notamment via l'Institut des Actuaires à développer des approches innovantes de modélisation du risque cyber des PME	P2	CT/MT
	- Renforcer la formation des intermédiaires d'assurance : dans le cadre la formation annuelle obligatoire liée à la DDA, prévoir l'inclusion obligatoire de modules portant sur le risque cyber	P1	CT
6	**Etudier des pistes alternatives**		
	- Continuer les réflexions autour d'un projet de *pool* d'assureurs / réassureurs dédié au risque cyber (dans la lignée du projet CATEX) avec la participation de l'Etat comme assureur de dernier ressort	P2	MT
	- Revoir les règles de calcul des provisions d'égalisation pour les assureurs pour les étendre au risque cyber	P2	CT/MT
	- Réfléchir à la mise en place de captives associant plusieurs PME (sur la base des captives par compartiment disponibles à Malte)	P3	MT

Glossaire

ACPR : Autorité de Contrôle Prudentiel et de Résolution

AGEA : Fédération nationale des syndicats à agents généraux d'assurance

AI : *Artificial Intelligence*, intelligence artificielle

AMRAE : Association pour le Management des Risques et des Assurances de l'Entreprise

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

APREF : Association des Professionnels de la Réassurance En France

BOFiP : Bulletin Officiel des Finances Publiques

CCI : Chambre de commerce et d'industrie

CESE : Conseil Economique Social et Environnemental

CESIN : Club des Experts de la Sécurité de l'Informatique et du Numérique

CNCC : Compagnie Nationale des Commissaires aux Comptes

CPME : Confédération des Petites et Moyennes Entreprises

CSIRT : *Computer Security Incident Response Team*, équipe de réponse aux incidents cyber

CSSF : Commission de Surveillance du Secteur Financier

DDA : Directive sur la distribution d'assurance

DDoS : *Distributed Denial of service*, déni de service distribué

Directive NIS (*Network and Information Security*) : Directive européenne sur la sécurité des réseaux et des systèmes d'information

EIOPA : *European Insurance and Occupational Pensions Authority*, autorité européenne des assurances et des pensions professionnelles

EMEA: *Europe, Middle East, and Africa*

ENISA : Agence européenne pour la cybersécurité

ETI : Entreprises de Taille Intermédiaire

FERMA : *Federation of European Risk Management Associations* - équivalent européen de l'AMRAE

Fevad : Fédération du e-commerce et de la vente à distance

GDV : *Gesamtverband der Versicherer* - équivalent allemand de France Assureurs

GIP ACYMA : Groupement d'Intérêt Public contre la Cybermalveillance

IA : Intelligence Artificielle

IAIS : *International Association of Insurance Supervisors*

IFRI : Institut Français des Relations Internationales

KYC: *Know Your Customer* (connaissance client)

LOPMI : Loi d'Orientation et de Programmation du ministère de l'Intérieur

MEDEF : Mouvement des entreprises de France

MGA : *Managing General Agent*, agent général principal

MOOC : *Massive Open Online Course*, cours en ligne ouvert à tous

OCDE : Organisation de coopération et de développement économique

OES : Opérateur Essentiel de Service

OIV : Opérateur d'Importance Vitale

Planète CSCA : Syndicat des courtiers d'assurance

PME : Petites et Moyennes Entreprises

Règlement DORA (*Digital Operational Resilience Act*) : règlement européen sur la résilience opérationnelle numérique

RGPD : Règlement Général sur la Protection des Données

RSSI : Responsable de la Sécurité des Systèmes d'Information

SaaS : *Software as a Service*, logiciel en tant que service

SLA : *Service Level Agreement*, accord sur les niveaux de service

U2P : Union des Entreprises de Proximité

Bibliographie

Etudes et rapports

- Allianz, "*Cyber: The Changing Threat Landscape*", octobre 2022
- Allianz, "*Cyber security trends 2023*", octobre 2023
- Allianz Global Corporate and Specialty, "Baromètre des risques 2023", janvier 2023
- Allianz, Axa HDI, Howden, Marsh, Lloyds, MunichRe, FERMA, "*How Can Europe Lead the Way to Cyber Resilience*", juin 2023
- AM Best, "*Market Segment Report: US Cyber: First Hard Market Cycle Brings a Return to Profitability*", 13 juin 2023
- AMRAE, "Etude LUCY" (LUmière sur la CYberassurance), 1ère édition, mai 2021
- AMRAE, "Etude LUCY" (LUmière sur la CYberassurance), 2ème édition, juin 2022
- AMRAE, "Etude LUCY" (LUmière sur la CYberassurance), 3ème édition, mai 2023
- ANOZR WAY, "Baromètre du *ransomware*, 5ème édition", janvier 2023
- ANSSI, "La Cybersécurité pour les TPE/PME en 12 questions", février 2021
- ANSSI, "Rapport d'activité 2021", mai 2022
- ANSSI, "Rapport d'activité 2022", avril 2023
- APREF, note de position "Assurance et réassurance du risque cyber", décembre 2021
- Assemblée nationale, "Compte-rendu - commission de la défense nationale et des forces armées", avril 2023
- Asterès, "Les Cyberattaques réussies en France : un coût de 2 Mds€ en 2022", juin 2023
- Bessé, « Crise cyber : quel impact sur les entreprises non cotées ? », novembre 2020
- Bessé, en partenariat avec Stelliant, "Risques cyber : analyse de la sinistralité : quels enseignements ?", octobre 2022
- M. Castellazzi, C. Duchesne-Jeanneney et I. Faucheux, « La Responsabilité des fournisseurs de systèmes numériques », Conseil général de l'économie, de l'industrie, de l'énergie et des technologies, juin 2020
- CCI Ile de France, "Pérenniser l'entreprise face au risque cyber", juin 2021
- CESE, "Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques", avril 2022
- Le Club des Juristes, "Assurer le risque cyber", janvier 2018
- Le Club des juristes, "Le Droit pénal à l'épreuve des cyberattaques", avril 2021
- Cybermalveillance.gouv.fr, "Rapport d'activité 2022", mars 2023

- Cyber Security Ventures, "*2022 Official Cybercrime Report*", décembre 2022
- Commission Européenne, "*Digital Economy and Society Index 2022*", juillet 2023
- Direction Générale du Trésor "Le Développement de l'assurance du risque cyber", septembre 2022
- EIOPA, "*Consultation paper on supervisory statement on management of non-affirmative cyber underwriting exposures*", mai 2022
- EIOPA, "*Strategy on cyber underwriting*", février 2020
- ENISA, "*Demand Side of Cyber Insurance in the EU*", février 2023
- ENISA, "*Threat Landscape 2023*", octobre 20223
- ENISA, "*Threat Landscape for Ransomware Attacks*," juillet 2022
- V. Faure-Muntian, Assemblée Nationale, Groupe d'étude Assurance, "Rapport sur la cyber assurance", octobre 2021
- Fédération Française de la Cybersécurité (en partenariat avec Apave, Itrust et Free Pro), "Enquête de maturité des TPE/PME françaises 2023", juillet 2023
- France Assureurs, étude statistique "L'Assurance de dommages aux biens des professionnels en 2022", juin 2023
- France Assureurs, "Cartographie prospective 2023 des risques de la profession de l'assurance et de la réassurance", janvier 2023
- FERMA, "*Position Paper on the European Commission's Cyber Resilience Act Initiative*", mai 2022
- FERMA, "*European Risk Manager Survey Report - 2022*", août 2023
- Hiscox Assurances, "Rapport 2023 sur la gestion des cyberrisques", 7ème édition, octobre 2023
- Hiscox Assurances, "Rapport 2022 sur la gestion des cyberrisques", 6ème édition, novembre 2022
- IAIS, "*Global Insurance Market Report - Special Topic Edition - Cyber*", avril 2023
- InCyber, "Baromètre fuite de données", mai 2023
- Insee, "Les Entreprises en France - édition 2022", décembre 2022
- Institut des Actuaires, "Note sur l'assurance paramétrique : cas particulier du risque cyber", 2021
- Institut Intermédius, *think tank* de Planète CSCA, "Risque cyber : "comment les cabinets de courtage de proximité peuvent-ils s'en prémunir et conseiller leurs clients", septembre 2023
- Institut Montaigne, "Cybermenace : avis de tempête", novembre 2018
- Institut Montaigne, "Cybersécurité : passons à l'échelle", juin 2023
- Institut Montaigne, "Industrie du futur, prêts, partez !", septembre 2018

- Institut Montaigne "Mobiliser et former les talents du numérique" mai 2023
- ISUNA, White Paper "*Cyber Insurance : Multistakeholder Challenges and Solutions*", septembre 2022
- Long Finance, "*Promoting UK Cyber Prosperity : Public-Private Cyber Catastrophe Reinsurance*", juillet 2015
- S. Marsaud et S. Rousseau, Assemblée Nationale, Comité d'évaluation et de contrôle des politiques publiques, "Rapport sur l'évaluation de la prise en compte du retrait-gonflement des argiles", mars 2023
- S. Meurant et R. Cardon, rapport d'information au Sénat fait au nom de la délégation des entreprises "La Cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?", juin 2021
- Munich Re, " *Cyber insurance : risks and trends 2023*", avril 2023
- Munich Re, "*Global Cyber Risk & Insurance Survey 2022*", août 2022
- NetDiligence, "*Cyber Claims Study 2023 Report*", 13ème édition, octobre 2023
- JC. Noël, "La Cyberpuissance israëlienne : l'essor inachevé de la *start up* nation ? », IFRI, novembre 2020
- Observatoire de la Filière de la Confiance Numérique, « Rapport annuel 2023 », juin 2023
- OCDE, "*Enhancing the Availability of Data for Cyber Insurance Underwriting. The role of public policy and regulation*", février 2020
- OCDE, "*Enhancing the Role of Insurance Cyber Risk Management*", novembre 2017
- OCDE, "*Unleashing the Potential of the Cyber Insurance Market*", février 2018
- Opinion Way pour le CESIN, "Baromètre de la cybersécurité des entreprises", 8ème édition, janvier 2023
- OpinionWay pour QBE, "Gestion des risques des PME et ETI en France", 6ème édition, février 2023
- T. Peyrat, "Risque cyber, un modèle épidémiologique sur réseaux pour le risque d'accumulation du cyber silencieux", mémoire de l'Institut des Actuaires, octobre 2023
- PwC, "*Cyber Threats 2022: A Year in Retrospect*", mai 2023
- *S&P, "Global Cyber Insurance : Reinsurance Remains Key to Growth"*, août 2023

Ouvrages

- Baruch Berliner, "*Limits of Insurability of Risks*", Prentice-Hall, 1982
- Michael Powers, "*Acts of God and Man*", Columbia Business School Publishing, 2012

- Michel Serres, “Petite Poucette”, Le Pommier, mars 2012

Articles de recherche

- C. Biener, M. Eling et JH Wirfs, “*Insurability of Cyber Risks: an Empirical Analysis*”, The Geneva Association et Institute of Insurance Economics at the University of St Gallen, août 2014
- RA. Carter, D. Pain et J. Enoizi, “*Insuring Hostile Cyber Activity : in search of sustainable solutions*”, The Geneva Association, janvier 2022
- M. Eling et JH. Wirfs, “*Cyber Risk: Too Big To Insure*”, University of St Gallen et Swiss Re, 2016
- M. Eling et W. Schnell, “*Ten Key Questions on Cyber Risk & Cyber Risk Insurance*”, The Geneva Association, novembre 2016
- MG. Fauré, “*The Limits of Insurability From a Law and Economic Perspective*”, The Geneva Papers on Risk and Insurance, juillet 1995
- S. Héon et D. Parsoire, “La Couverture du cyber risque”, The Geneva Papers on Risk and Insurance, février 2017
- O. Lopez et F. Picard, “Cyber-assurance : nouveaux modèles pour quantifier l’impact économique des risques numériques”, mars 2019

Articles, communiqués de presse et ressources internet

- ACPR, communiqué de presse “Garanties implicites contenues dans les contrats en matière de couverture du risque cyber”, 23 septembre 2022
- ACPR, communiqué de presse “La Distribution des garanties contre les risques cyber par les assureurs”, 12 novembre 2019
- ANSSI, https://www.ssi.gouv.fr et https://secnumacademie.gouv.fr/ (accès aux MOOC)
- L’Argus de l’Assurance, “Courtage : April s’ouvre à l’assurance cyber”, 18 octobre 2023
- L’Argus de l’Assurance, “Les réassureurs avancent à l’aveugle sur le cyber”, 11 octobre 2023
- L’Argus de l’assurance, “Risque cyber : pourquoi les PME ne s'assurent (toujours) pas”, 28 juin 2023
- Beazley, communiqué de presse “*Beazley launches market’s first cyber catastrophe bond*”, 9 janvier 2023

- BOFiP, https://bofip.impots.gouv.fr/bofip/2444-PGP.html/identifiant%3DBOI-TCAS-ASSUR-10-40-50-20210407
- BoostAeroSpace (*cloud* privé de l'industrie européenne de l'aérospatiale et de la défense), *https://boostaerospace.com/aircyber/*
- BPI France, communiqué de presse « Cybersécurité : Bpifrance poursuit son ambition d'accompagner les entreprises dans la prévention de ce risque et lance le « Diag Cybersécurité » », 20 mars 2023
- Business Insurance, "*Axis Capital sponsors $75 million cyber cat bond*", 19 octobre 2023
- Centre for Cyber security Belgium, *https://ccb.belgium.be/en/cyberfundamentals-framework*
- CNCC, https://www.cncc.fr/a-vos-outils/
- Conseil national de la sécurité routière, https://conseilnational-securiteroutiere.fr/le-cnsr/#le-cnsr-en-bref
- Cybermalveillance.gouv.fr, www.cybermaveillance.gouv.fr
- Les Echos, "Cyberattaques : les PME en première ligne du risque numérique", 11 octobre 2023
- Les Echos, "*Insurtech* : la data au service du *risk management*", 1er février 2023
- Les Echos, "Les très petites entreprises ont une mauvaise image des organisations patronales nationales", 26 juin 2023
- EIOPA, communiqué de presse "*EIOPA launches survey on access to cyber insurance by SMEs*", 20 septembre 2023
- Emisoft, "*Unpacking the MOVEit Breach: Statistics and Analysis*", données au 26 octobre 2023
- Feel Agile, https://feelagile.com/accompagnement-iso-27001/
- Fevad, communiqué de presse « Baromètre de l'audience du e-commerce : 2ème trimestre 2023 », 27 septembre 2023
- France Assureurs, www.franceassureurs.fr/nos-positions/lassurance-qui-protege/projet-catex/
- France Num, www.francenum.gouv.fr/partenaires/
- *Gesamtverband der Versicherer* (fédération allemande de l'assurance), *www.gdv.de/gdv/themen/digitalisierung/initiative-cyber-sicher*
- Gouvernement, communiqué de presse "Cédric O présente le nouveau dispositif d'alerte des entreprises en cas d'incident majeur", 20 juillet 2021
- Gouvernement, secrétariat général du Comité interministériel de prévention de la délinquance et de la radicalisation, www.cipdr.gouv.fr/le-cipdr/le-fipd

- Gouvernement britannique, *www.gov.uk/government/publications/cyber-essentials-scheme-overview*
- Insurer Intelligent*, "Parametric cyber: turning the market on its head"*, 27 mars 2023
- Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, https://www.economie.gouv.fr/facileco/assurance-assureurs-mediation
- Ministère de l'intérieur, communiqué de presse "En 2021, comme tous les ans, l'effort financier de l'État en faveur de la sécurité routière (3,7 milliards d'euros par an) est plus de quatre fois supérieur aux recettes des radars automatiques (859 M€ en 2021)", 13 octobre 2022
- Sécurité et Défense magazine, « Tour du monde de la sécurité : des approches diverses », 15 juin 2023
- The Wall Street Journal*, "Smaller Companies Are Urged to Adopt Multi Factor Authentication"*, 5 juillet 2022
- Wavestone, communiqué de presse « Maturité cyber en France : une progression notable dans les grandes organisations qui se ressent sur la réussite des cyberattaques », 18 avril 2023

Lois et textes réglementaires

- Code de la consommation, article L212-1 : https://www.dalloz.fr/documentation/Document?id=CCSM000449
- Code de la consommation, article L221-3 : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000019749595#:~:text=a)%20Provision%20destin%C3%A9e%20%C3%A0%20faire,li%C3%A9s%20aux%20attentats%20et%20au
- *Cyber Resilience Act* : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
- Décret sur la définition des PME (dans le cadre de la loi sur la modernisation de l'économie) : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000019961059/
- Directive sur la Distribution de l'Assurance : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32016L0097
- Directive NIS 1 : https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32016L1148
- Directive NIS 2 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022L2555

- Loi d'Orientation et de Programmation du ministère de l'Intérieur : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768
- Loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034290626/
- Règlement DORA : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020PC0595

Résumé

<u>Mots clés</u> : PME, risque cyber, cyberattaque, assurance cyber, cybersécurité, cyber-résilience.

Une PME française sur 2 a été victime d'une cyberattaque en 2022 selon plusieurs études. Pourtant les PME françaises ne sont qu'une infime minorité à avoir souscrit une assurance cyber.

Cet apparent paradoxe nous a conduit à nous interroger sur les raisons qui expliquent la situation actuelle. Les freins existent du côté de l'offre (assurance cyber encore méconnue, perçue comme complexe et chère) mais surtout du côté de la demande. Les dirigeants de PME sous-estiment encore le risque cyber et, quand ils y sont sensibilisés, ils manquent de moyens et se trouvent désarmés face à la multitude d'acteurs et d'outils disponibles.

Nous recommandons donc que l'Etat fasse de la cybersécurité des PME une de ses causes prioritaires, avec notamment une campagne massive de sensibilisation au risque. L'autre priorité est d'accompagner les PME vers la cybersécurité avec un "guichet unique", un référentiel commun de cybersécurité et une aide financière.

Le secteur de l'assurance, qui a toujours su accompagner les évolutions de la société, a aussi son rôle à jouer en améliorant la lisibilité et la comparabilité des offres, et en créant des offres adaptées aux PME associant prévention, couverture et assistance.

La cyber-résilience des PME françaises est un enjeu majeur pour l'économie et la sécurité nationale et sollicite la mobilisation de tous les acteurs.