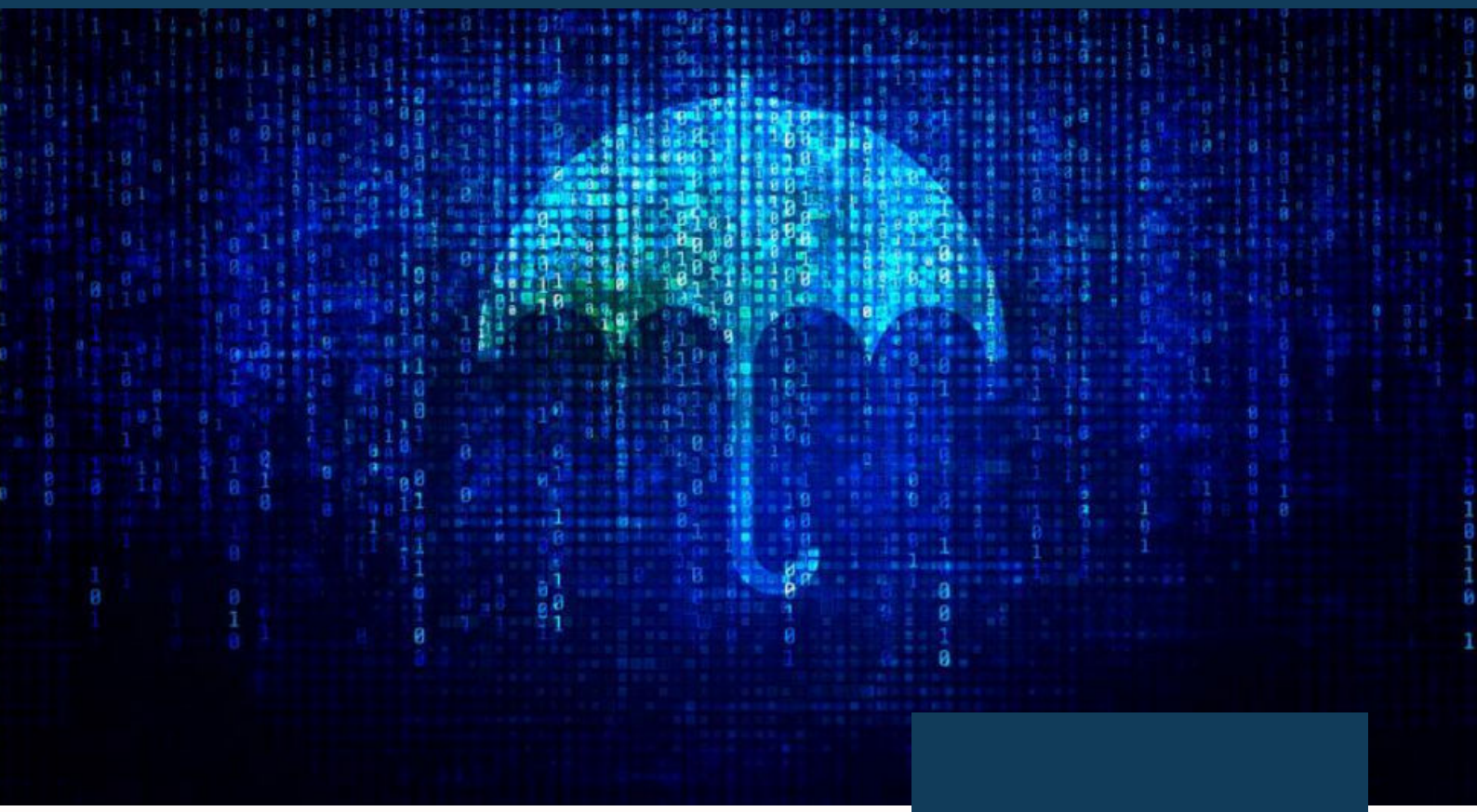
DECEMBRE 2021 | VOL. 7

Mag'Assur

Le bulletin d'information officiel du secteur Assurance



Septième édition de la Newsletter Assurance

Edito

Écrit par Sarah Madou

Et si un virus pouvait en cacher un autre ? Depuis le début de la pandémie COVID-19, la mise en œuvre du travail à distance, qui a permis d'assurer la continuité d'activité pour beaucoup d'entreprises pendant les périodes de confinement successives, n'a pas été sans risques au niveau de la sécurité des systèmes d'informations de ces dernières. Malgré lui, le télétravail a mis en lumière certaines failles de sécurité du parc informatique ainsi que le besoin de compétences cyber des organisations françaises et internationales. Il ne se passe pas une semaine sans qu'une entreprise, une collectivité ou encore une association ne soit victime d'une cyberattaque par l'un des groupes de hackers Ryuk, Egregor, Networker, REvil ou DoppelPaymer. Cette tendance n'est pas prête de s'arrêter.

Que ce soit par la mise en place de protocoles de sécurité plus performants, la sensibilisation à la cybersécurité des salariés ou encore des alliances entre les différents acteurs (gouvernement, acteurs de la tech, entreprises et assurances), la définition commune de "gestes barrières" cyber devient primordiale et d'intérêt national afin d'éviter que le risque "cyber" ne se transforme en nouvelle pandémie.

Nominations

- Après avoir intégré April en tant que directeur de la stratégie du groupe en 2021, Philippe Arnaud a pris la direction générale d'April Santé Prévoyance depuis le 1er novembre 2021.

- Actuellement Directeur Général d'AXA Allemagne et membre du comité exécutif du groupe depuis 2016, Alexander Vollert deviendra, à compter du 1er décembre 2021, le Directeur des Opérations du Groupe AXA.
- Il sera remplacé par Thilo Schamacher (sous réserve de l'approbation des autorités réglementaires).
- Côté AXA XL, Andy MacFarlane officie maintenant à la position de Head of Climate, où il sera chargé de développer la stratégie climat d'AXA XL à l'échelle mondiale.

- Eric Chenut a été élu à la présidence de la Mutualité Française pour un mandat de 5 ans le 5 octobre 2021. Il succède à Thierry Beaudet qui prend la présidence du Conseil économique social et environnemental.

- Sébastien Seux succède à Olivier Muraire à la direction générale d'Axeria IARD six mois après la cession d'Axeria IARD à Watford.

- Dans le cadre de la réorganisation des équipes EMEA chez AON courant septembre 2021, Robert Leblanc a été nommé à la présidence d'AON EMEA.
- Il a été rejoint, deux semaines plus tard, par Laurent Belhout, qui a pris la position de CEO d'Aon France-Belgique-Luxembourg-Maroc.

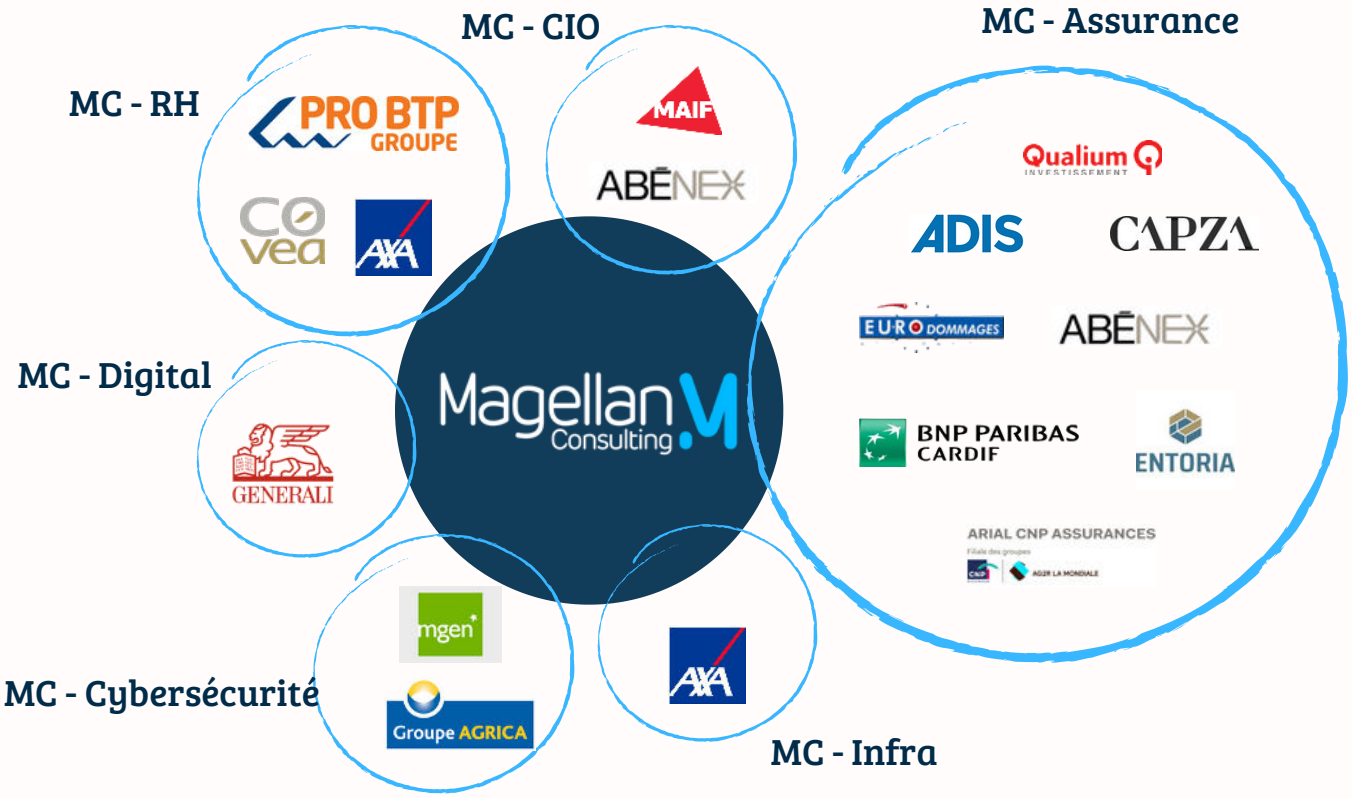
- Nathalie Couveignes a intégré au 1er septembre 2021 la France Mutualiste comme directrice du développement omnicanal. Au sein du groupe mutualiste, elle pilote l'ensemble des canaux de distribution, du marketing produits et digital, de la communication et de l'engagement.
- Elle est suivie de Christelle Le Berre qui a rejoint la France Mutualiste comme directrice générale adjointe de Média Courtage et directrice des synergies entre Média Courtage et la France Mutualiste.

Rapprochements

La direction de la concurrence de la commission européenne a donné son accord pour le projet de rapprochement entre le groupe Siaci Saint Honoré et le courtier Diot. S'ils reçoivent l'accord des autorités réglementaires au Luxembourg et au Moyen Orient, le groupe deviendra le numéro un français du courtage d'assurance et le 5ème courtier sur la scène européenne.

SMACL Assurances (soutenu par le Groupe VYV) et le Groupe MAIF se rapprochent et créent une société d'assurance commune au service des collectivités territoriales, SMACL Assurances SA. Cette nouvelle société prendra ses fonctions au 1er janvier 2022 (sous réserve d'un avis favorable des autorités de contrôle compétentes).

Missions en cours



INSTANT TECH

Assurup

Fondée en 2015, ce courtier et startup veut dépoussièrer et simplifier le processus d'assurance des entreprises et des salariés dans le cadre de travail sur et hors site. De la responsabilité civile en passant par le risque cyber et le téletravail, Assurup s'adresse principalement aux startups et scale-ups.
EN SAVOIR PLUS

At Bay

Cette start-up canadienne veut révolutionner l'assurance cyber en alliant à la fois couverture cyber et accompagnement dans la réalisation d'une politique de cyber sécurité pérenne. En quelques mots, At Bay propose d'évaluer les cyber-risques de ses entreprises clientes et leur soumettre des recommandations pour améliorer leur cybersécurité (avec des tarifs de police plus avantageux si elles les appliquent). EN SAVOIR PLUS

Kovrr

La plate-forme Kovrr (start-up israélienne) a été conçue pour aider les souscripteurs, les gestionnaires d'exposition et les modélisateurs de catastrophes à comprendre, quantifier et gérer les cyber-risques en utilisant des modèles de risque prédictifs basés sur l'IA. Kovrr compte parmi ses clients AON. EN SAVOIR PLUS

LE RISQUE CYBER

TOUR D'HORIZON

Écrit par Bertrand Bickelmann, Nadia Maatar, Sarah Madou et Mohamed Taha Taboubi

Nous l'évoquions dans notre newsletter du bilan de l'année 2020, aujourd'hui toutes les entreprises quel que soit leur secteur d'activité ou leur taille sont susceptibles d'être touchées par une cyber-attaque (y compris les assureurs). Aux vues du faible taux d'équipement, on peut dire que le marché français de la cyber assurance en est encore à ses balbutiements. Mais les assureurs se doivent de vanter les bienfaits de leurs offres de cyber assurance et l'aide apportée à leurs clients face à un problème trop souvent géré dans l'urgence, non anticipé, non préparé et pouvant avoir des conséquences dramatiques sur les plans financiers, techniques et d'image.

Contexte

Dans son rapport annuel 2021, le groupe Hiscox assurances met en avant qu'entre 2020 et 2021, notamment du fait de la pandémie et du développement du télétravail, le nombre d'attaques visant les entreprises françaises a augmenté (49% des participants à l'enquête signalaient avoir été victime d'au moins une cyber attaque versus 34% l'année précédente). Force est de constater qu'aujourd'hui toutes les entreprises représentent des victimes potentielles. L'imagination des hackers est prolifique et les types d'attaques sont multiples (liste non exhaustive) :

- Installation de programmes espions et de programmes pirates
- Phishing
- Dénis de service sur des sites
- Intrusions
- Vol d'informations
- Ransomware ...

Pour se défendre les entreprises ont augmenté leurs dépenses en cybersécurité (20% de dépenses informatiques allouées à la cybersécurité en 2021 contre 13% en 2020) alors que, parallèlement la souscription d'une garantie cyber-risques progresse plus lentement. Aujourd'hui, tout l'enjeu des acteurs de l'assurance est de démontrer les bienfaits de ce type de produit afin d'en accroitre sa détention et d'en faire un instrument aussi indispensable qu'une assurance professionnelle.

Dans son rapport sur la cyber assurance, la députée Valeria Faure-Muntian propose de dynamiser le marché à travers des propositions visant à renforcer les moyens de l'Etat dans la lutte, sensibiliser les acteurs, harmoniser les règles cyber européennes (des mesures également évoquées par l'autorité de régulation), rapprocher assureurs français et entreprises de cybersécurité françaises.

Pourquoi on en parle ?

Face à une augmentation considérable de la cybercriminalité (+ 225% des signalements d'attaques par rançongiciels par rapport à 2019 selon l'ANSSI[1]) et face à une évolution permanente de nouvelles technologies, souscrire à une police d'assurance cyber risque devient une protection indispensable.
Les grands groupes sont assurément saisis du risque et sont de plus en plus nombreux à souscrire à ces assurances. Selon le baromètre annuel du CESIN[2], 60% des entreprises ont souscrit une cyber assurance en 2020 contre 10% l'année précédente, 13% sont en train de le faire et 11% envisagent de souscrire à plus long terme.
Les entreprises de taille plus modeste, les collectivités territoriales et les administrations sont quant à elles moins enclin à souscrire à ces assurances cyber et se retrouvent plus vulnérables et plus fragiles face à ces cybers attaques qui se multiplient.

[1] ANSSI (Agence Nationale de Sécurité des Systèmes d'Information)
[2] CESIN (Club des Experts de la Sécurité de l'Information et du Numérique)

Et quels bénéfices?

Dans ce contexte, le secteur des assurances s'est imposé comme un vecteur indispensable de la prévention et de la lutte contre les cybers attaques. La souscription à une cyber assurance offre de nombreux avantages pour l'entreprise :

Accompagnement dans la prévention des cyber attaques :

- Réalisation d'audits et recommandations
- Tests d'intrusion
- Acculturation et formations

Accompagnement dans la gestion de crise en cas d'attaque :

- Accompagnement dans les procédures et premières actions à mettre en place pour limiter les conséquences de la cyber attaque
- Mise à disposition d'experts en analyse forensic pour comprendre ce qui s'est passé et éviter les futures attaques
- Accompagnement sur la communication (réhabilitation de l'image, relations publiques)
- Indemnisation des préjudices financiers, juridiques et réputationnelles (pertes d'exploitation, frais juridiques, autres coûts conséquents…)

Responsabilité civile sur les attaques cyber (non pris en charge par les RC Pro) :

- Perte et diffusion massive des données personnelles / confidentielles
- Atteinte au respect de la vie privée et aux droits de la personnalité
- Atteinte à la sécurité du réseau

Quelle est la situation à ce jour?

87%
des grandes entreprises

8%
des entreprises de taille intermédiaire **ont souscrit à une assurance cyber en 2020**

167% vs 84%
ratio Sinistres/Primes de 2020 vs celui de 2019

38 M€
hauteur moyenne de **couverture des grandes entreprises** en 2020

79 %
Phishing ou spear-phishing

47%
Arnaque au Président **sont les principaux vecteurs d'attaques constatées**
(suivies de près par l'exploitation d'une vulnérabilité et les tentatives de connexion)

+ 19%
pour les grandes entreprises

+ 28%
pour les ETI
Augmentation des taux de primes entre 2019 et 2020

35 %
Usurpation d'identité

34%
Infection par un malware **sont les conséquences majeurs les plus fréquentes**

Source : AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise), 2020

Oeil critique de Magellan

Les assureurs, qu'ils soient dynamiques ou attentistes, demeurent prudents face à ce risque évolutif, polymorphe et dont le terrain de jeu est encore inexploré. Les principales complexités que nous identifions sont :

Modélisation difficile du risque cyber	• Absence d'une définition commune et partagée du risque Cyber. • Manque des données sur l'historique des sinistres. • Sinistralité sous-estimée en l'absence de déclaration systématique des attaques et la réticence des entreprises à partager sur les impacts relatifs. • Evolution incessante et rapide des techniques de cyberattaque et de nouvelles technologies
Un marché à deux vitesses	• Manque d'offre sur le marché des grandes entreprises avec un niveau de couverture proposée qui ne correspond pas à leurs besoins réels • Faible demande sur le marché des ETI et PME, qui est fortement freinée par le niveau de maturité et d'information de ces structures (démarches en interne sur la cybersécurité et les réflexions autour d'un éventuel transfert de risque aux assurances)
Estimation épineuse des coûts	• En France, il a suffi d'avoir quatre incidents de taille pour faire pencher la balance et tripler le montant des indemnisations (de 73 millions d'euros en 2019 à 217 millions d'euros en 2020). D'après l'assurance américaine « Chubb », on note une hausse des primes autour de 30% en 2021 (par rapport aux primes de 2020) mais qui devrait atteindre les 100% en 2022.

L'avenir du Cyber Risque ?

La couverture par un contrat cyberassurance est désormais soumise à des conditions de cyber-hygiène, devenant de plus en plus exigeantes. Les entreprises ayant un niveau de risque élevé se trouvent contraintes de payer des primes accablantes.

Face à ce constat, ces entreprises vont chercher à améliorer leurs dispositifs de cybersécurité pour bénéficier des tarifs plus intéressants. La mise en place d'une bonne cybersécurité, via l'adoption massive de certifications et normes de sécurité au sein des entreprises, **tels que la suite ISO (27K notamment), SecNumCloud ou encore l'authentification Multifacteur du côté des entreprises** faciliterait le processus de cyberassurance à plusieurs niveaux :

Assouplissement du processus d'obtention de couverture

Baisse mécanique des primes

Supression des obstacles à l'indemnisation *(pendant la prise en charge)*

Pour développer ce marché, plusieurs pratiques pourraient être envisagées à l'avenir par les différentes parties prenantes (autorités publiques, assureurs, entreprises).

GOUVERNEMENT

- Adopter, en collaboration avec les acteurs du marché, des initiatives qui visent à sensibiliser les petites et moyennes entreprises aux cyberassurances pour mieux appréhender l'apport potentiel de celles-ci. Par exemple, le gouvernement anglais a élaboré, en ce sens, un guide pratique à l'attention des PME : « Making Sense of Cyber Insurance : a Guide for SMEs »
- Standardiser les offres en vue de s'assurer que celles-ci couvrent à minima certains risques essentiels (modèles de contrats, définitions et terminologies homogènes et communes, couverture de risques…).
- Soutenir des mécanismes de certification ou de label des produits cyberassurances

ACTEURS DU MARCHÉ

- Créer un dispositif de partage des données sur les cyberincidents qui se sont produits. Le partage d'informations provenant de sources multiples et organisées par secteur et par type d'attaque permettra aux compagnies d'assurance de mieux calculer leurs primes, stabiliser davantage le modèle assurantiel et proposer des contrats en adéquation avec les besoins réels du marché.

Pour conclure, il ne faut pas oublier que la cyberassurance ne devrait traiter que les risques résiduels et ne peut en aucun cas se substituer aux mécanismes cybersécurité des entreprises. Tous les acteurs de cette chaîne de valeur doivent travailler collectivement au développement de ce marché qui peine, pour l'heure, à atteindre sa vitesse de croisière.

LEXIQUE

Phishing	Technique de piratage de masse utilisant l'usurpation d'identité afin d'obtenir des renseignements sensibles tels que les noms d'utilisateurs, les mots de passe ou les détails de carte de crédit.
Spear-phishing	Le spear-phishing se différencie du phishing par son spectre. L'usurpation d'identité est ciblée, l'identité usurpée peut être un fournisseur, un client, ou un collaborateur direct.
Ransomware	Prise en otage des données personnelles afin de demander le versement d'une rançon en échange de la clef de chiffrement des données cryptées.
Arnaque au Président	Usurpation d'identité d'un membre de direction afin de demander le versement, souvent rapide et urgent, d'une somme d'argent sur un compte à l'étranger. Les principales cibles sont les services comptables et secrétariats de direction.
Malware	Terme générique pour tout logiciel catégorisé comme malveillant (logiciel espion, cheval de Troie, ver informatique, etc.).

LA REVUE DE PRESSE

01 Quoi de neuf chez les acteurs de l'assurance ?!

AXA appelle l'état à créer des alliances entre le public et le privé

AXA tire à nouveau la sonnette d'alarme pour le développement d'une réponse commune public / privé sur les incidents cyber majeurs et risques systèmiques. Cet appel fait suite à la présentation d'un rapport sur les risques futurs élaboré fin septembre 2021, où le risque cyber arrive en tête de liste. EN SAVOIR PLUS

Le secteur de l'assurance n'est pas épargné par les cybercriminels, et AssurOne, courtier grossiste, en a fait les frais au mois d'août 2021

Victime d'une tentative de ransomware sur un de ses serveurs, la société de courtage a très vite réagi pour stopper la tentative d'intrusion. Après une semaine de nettoyage et 2/3 jours d'arrêt d'activité, la société de courtage a pu reprendre son activité à 90% bien que la faille de sécurité n'ait pas été identifiée. EN SAVOIR PLUS

La Mutuelle Générale s'arme pour la cybersécurité

Afin de lutter contre les cyberattaques, en particulier les ransomwares, la Mutuelle Générale s'allie avec BlueTrusty, la filiale cybersécurité de l'entreprise de services du numérique ITS Group, pour évaluer la résistance de ses postes de travail au ransomware. EN SAVOIR PLUS

02 Le métier de l'assurance dans tous ses états

L'ACPR encourage les assureurs à se protéger contre la cybercriminalité

Face à la recrudescence des cyberattaques, l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) a émis 25 recommandations à l'attention des assureurs. Elle incite le secteur à se doter d'outils pour se prémunir contre un tel risque. EN SAVOIR PLUS

Tensions autour du risque cyber suite à la crise COVID-19

Selon Gras Savoye Willis Towers Watson, la crise sanitaire aurait amplifié le durcissement du marché de l'assurance. Le risque cyber serait le marché le plus impacté par les redressements, au risque de détruire l'intérêt pour cette couverture, devenue indispensable. EN SAVOIR PLUS

Débats autour du paiement des rançons par les compagnies d'assurance

Dans un rapport parlementaire contenant 20 propositions pour la cyber-assurance, Valéria Faure-Muntian suggère d'inscrire l'interdiction de garantir, couvrir ou indemniser la rançon. EN SAVOIR PLUS

Nous travaillons ou avons travaillé avec ces acteurs de l'assurance

Nos offres

TRANSFORMATION MÉTIER

Adapter la stratégie assurantielle pour anticiper les défis et enjeux de demain

- Nouveaux acteurs (insurtech)
- Disruption
- Nouveaux risques
- Stratégie RSE et ESG
- Nouveaux business models
- Partenariats

UX/CX

Remettre le client au centre de vos intérêts et créer l'expérience client

- Parcours clients
- Relation clients
- Omnicanalité
- Services clients / selfcare

DATA STRATEGY

Remettre la data au coeur du business model de l'assurance car elle l'a créée

- Gouvernance
- Data driven disruption
- Data management platform
- Security
- Data analysis

TRANSFORMATION DES ORGANISATIONS

Tirer profit des nouvelles technologies pour améliorer l'agilité des organisations

- Concentration du secteur
- Optimisation des processus
- Automatisation
- Transformation technologique
- Stratégie de plateformes

COMPLIANCE

Transformer la contrainte en opportunité

- Protection de la clientèle
- Réglementaire prudentiel (Solvabilité II, ICS)
- Réglementaire financier (IFRS, Lois de Finance)
- Cybersécurité
- Contrôle interne

Equipe de rédaction

Bertrand Bickelmann
Manager

Cécile Flament
Principal

Nadia Maatar
Consultante Senior

Sarah Madou
Consultante Senior

Fabrice Smadja
Senior Manager

Mohamed Taha Taboubi
Manager

Hans Willert
Associé

Envie d'aller plus loin à nos côtés ?

Nous avons hâte de donner à vos projets de transformations digitales le cadre qu'ils méritent pour prendre vie. La solution idéale existe, et nous l'imaginerons à vos côtés.

Nous contacter