2023

Cybersécurité : un risque immatériel bien tangible

place escange
Le think tank du risque immatériel en entreprise

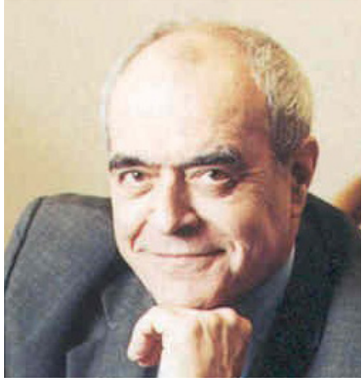
www.place-escange.fr

Ce guide, à destination des entreprises, aborde de façon pragmatique l'ensemble des aspects de la cybersécurité. C'est le résultat d'un travail réalisé par « Place Escange » en collaboration avec **Jean-Noël Barrot,** Ministre délégué chargé de la Transition Numérique et des Télécommunications, **Nicolas Arpagian,** Directeur de la Stratégie en cybersécurité de Trend Micro Europe, Enseignant à l'Ecole Nationale Supérieure de la Police et à Science Po Saint Germain en Laye, **Alain Juillet,** Président d'Honneur de l'Académie de l'Intelligence Economique, **Thibault Lanxade,** Entrepreneur et Président-Directeur Général du Groupe Luminess, **Jérôme Notin,** Directeur général du GIP ACYMA cybermalveillance.gouv.fr et **Michel Van Den Berghe,** Président de Campus Cyber, et bien d'autres experts.

Merci à eux pour leur apport éclairé sur le sujet.

Jean-Noël Barrot,

Nicolas Arpagian,



Alain Juillet,

Thibault Lanxade,

Jérôme Notin,

Michel Van Den Berghe

SOMMAIRE

LinkedIN : @place-escange

Twitter : PlaceEscange

ÉDITORIAL

Faut-il encore le rappeler ? Aujourd'hui, 80% des risques en entreprise sont immatériels… Une domination d'autant plus importante à prendre en considération que ces risques sont protéiformes : risque sanitaire, risque politique, cyber risque, risque des délais de paiements, risque géo-politique, risque de e-réputation…

Pour accompagner les entreprises dans l'identification, la compréhension et la gestion de ces risques, Place Escange, le think tank dédié au patrimoine immatériel des entreprises et à ses risques associés, publie régulièrement de nombreuses tribunes, podcasts, vidéos… sur son site place-escange.fr. Ce guide sur le risque cyber s'inscrit dans cette démarche.

Notre focus sur ce risque n'est pas le fruit du hasard. Depuis quelques années, le risque cyber connait une progression exponentielle notamment portée par l'évolution des entreprises et en particulier par leur transformation digitale et leur ouverture au monde de l'Internet. Or, si un temps les entreprises parvenaient à le contenir, force est de constater que la crise Covid a changé la donne sur le sujet : aujourd'hui, le risque cyber peut conduire à leur perte. Ce n'est d'ailleurs pas pour rien qu'il représente actuellement leur principale préoccupation.

Cet ouvrage a donc pour vocation de sensibiliser, alerter, conseiller sur les enjeux liés aux menaces issues du monde du net, afin que les entreprises s'en prémunissent le mieux possible.

Sa réalisation a notamment été rendue possible grâce à l'aide et au soutien du Ministre délégué chargé de la Transition numérique et des Télécommunications, Jean-Noël Barrot, de nos deux membres d'honneur Alain Juillet et Thibault Lanxade, des dirigeants du GIP ACYMA cybermalveillance.gouv.fr et du Campus Cyber, et d'autres experts… que nous remercions chaleureusement.

Ce guide se veut être le premier d'une série. En effet, pour demain, notre feuille de route ne varie pas et nous entendons poursuivre nos travaux notamment en publiant d'autres guides sur l'immatériel pour aider et accompagner les entreprises et en réfléchissant sur des notes de prospectives.

Charles Battista,
Président de Place Escange

Introduction

Désormais en tête des préoccupations de nombreuses entreprises et collectivités, le risque cyber fait de plus en plus l'objet de toutes les attentions dans les entreprises. Et pour cause, les « incidents cyber » se placent en tête des différentes études portant sur les risques des entreprises. Selon le Baromètre des risques d'Allianz 2023, la cybersécurité représente ainsi le premier sujet d'inquiétude des dirigeants français (40%).

La prise de conscience semble donc enfin avoir eu lieu et les entreprises se penchent de plus en plus sur leur sécurité numérique. Pour autant, face à l'accélération et à la complexification des attaques cyber, elles vont néanmoins devoir pousser un cran plus loin leurs démarches et renforcer leur stratégie de prévention et de maitrise de ces risques.

Au-delà des entreprises, les pouvoirs publics ont également un rôle important à jouer. Porté par les initiatives européennes, le régulateur français s'attache ainsi à légiférer pour protéger autant que possible les entreprises, en particulier contre ce risque. De même, l'état renforce ses dispositifs d'accompagnement des entreprises et collectivités face aux risques cyber.

Néanmoins, des efforts et des investissements restent à faire, notamment en termes de recherches et de formations, pour que la France dispose des ressources, compétences et expertises nécessaires au développement, à la compréhension et à l'exploitation des solutions propres à lutter efficacement contre le risque cyber.

1 ETATS DES LIEUX

Le numérique qui s'est invité dans le quotidien de tous, continue d'ouvrir la voie à des actes malveillants toujours plus sophistiqués et dont les impacts peuvent s'avérer fortement préjudiciables, voir fatals pour les entreprises visées.

A | Le risque cyber corrélé à la digitalisation de l'économie

Pour ceux qui peuvent encore en douter, le numérique et son environnement sont devenus des évènements essentiels de la civilisation moderne. Cependant, bien qu'étant source d'opportunités et vecteur majeur d'innovations, la transformation numérique s'accompagne également de nouvelles vulnérabilités. *« Aujourd'hui, il n'est plus possible d'exister dans notre civilisation moderne sans utilisation de toutes les facettes du numérique,»* **explique Alain Juillet, Président d'honneur de l'Académie de l'Intelligence Economique.** *« Cela implique d'en comprendre le fonctionnement et de l'intégrer dans notre environnement qui est d'une agressivité croissante. Plus ces systèmes sont efficaces et nous permettent de travailler, plus ils représentent un danger en termes de sécurité des échanges et d'utilisation frauduleuse des données. C'est la raison pour laquelle nous ne devons pas nous étonner des attaques cyber que nous subissons et des pratiques dont nous souffrons : ce sont désormais des composantes de ce nouveau monde ».*

Cette nouvelle dépendance du tissu économique au numérique ainsi que la rapidité de la transition digitale qui s'opère depuis quelques années ont ainsi facilité la multiplication de dommages ayant une origine cyber, en particulier les cyberattaques. La crise sanitaire a encore accéléré cette tendance, notamment à travers l'adoption de nouveaux modes de travail.

« Si auparavant nous pouvions dire que le risque cyber était essentiellement lié à des enjeux géopolitiques ou à l'intérêt de grandes puissances, aujourd'hui, il s'agit également d'un risque de proximité auquel tout un chacun est exposé », **précise ainsi Nicolas Arpagian, Directeur de la stratégie en cybersécurité de Trend Micro Europe et enseignant à l'Ecole Nationale Supérieure de la Police (ENSP) et à Sciences Po Saint Germain en Laye**.

B | Evolution exponentielle des cyberattaques

Selon une étude OpinionWay pour le CESIN, 54% des entreprises déclarent ainsi avoir subi au moins une attaque en 2021. Plus d'une entreprise sur deux est donc touchée. Des chiffres que corroborent le rapport Hiscox 2022, selon lequel 52 % des entreprises françaises auraient subi au moins une cyberattaque en 2022 (contre 49% en 2021).

Gage de la réalité de cette tendance, la plateforme cybermalvaillance.gouv.fr, chargée d'assister les victimes d'actes cyber malveillants, enregistre une augmentation de sa fréquentation depuis sa création « *Notre plateforme a ainsi reçu 1.4 millions de visiteurs en 2020, puis 2.4 millions en 2021 et près de de 3.8 millions en 2022*», **précise Jérôme Notin, Directeur général du GIP ACYMA cybermalveillance.gouv.fr.**

52%

DES ENTREPRISES FRANÇAISES AURAIENT SUBI AU MOINS UNE CYBERATTAQUE EN 2022

Jean-Noël Barrot,
Ministre délégué chargé de la Transition Numérique et des Télécommunications

> La menace cyber est ainsi passée du statut de l'exception à celui du quotidien et elle croit d'année en année en France. En 2021, il y a ainsi eu une augmentation de 37% des intrusions avérées dans des systèmes d'informations supervisées par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information). Chaque jour dans notre pays, ce sont près de 500 victimes (particuliers, collectivités, entreprises) qui font une demande d'assistance sur le site cybermalveillance.gouv.fr et nous assistons à 7 attaques sophistiquées contre des cibles critiques. Enfin, l'année dernière, une entreprise sur deux et une collectivité sur trois a déclaré avoir subi une attaque.

C | Des typologies d'attaques toujours plus sophistiquées

Le cyber risque renvoie à l'ensemble des risques liés à l'usage des technologies numériques et peut être défini comme un risque opérationnel portant sur la confidentialité, l'intégrité ou la disponibilité des données et des systèmes d'information. Il recouvre à la fois des actes malveillants mais aussi les incidents non intentionnels issus d'erreurs humaines ou d'accidents. Les outils et méthodes utilisés pour ces attaques sont en constante évolution. Il semblerait d'ailleurs que le recours au télétravail ait modifié les axes d'attaques.

Selon l'étude Opinionway pour le CESIN, les vecteurs d'attaques les plus répandues en 2021 restent le phishing (73%) et l'exploitation des failles, à savoir la vulnérabilité logicielle ou le défaut de configuration (53%). Viennent ensuite l'arnaque au président (38%), les tentatives de connexion (34%), les acquisitions de noms de domaines illégitimes (31%) ou encore les Ddos, attaque en déni de service (25%). Les attaques indirectes par rebond, via des prestataires, tendent également à augmenter (21% vs 16% en 2019), ce qui souligne la dépendance grandissante des entreprises envers leurs fournisseurs externes. « *Il est à ce titre important de veiller à la sécurisation des sites qui hébergent les données des entreprises*», **souligne Thibault Lanxade, Entrepreneur et Président-Directeur Général du Groupe Luminess**. « *Par exemple chez Luminess, nous sommes dans une logique de souveraineté numérique : nos sites d'hébergement se trouvent à Mayenne et Laval* ».

D | Les points d'entrée des attaques

Vulnérabilité créée par l'erreur humaine

Le premier point d'entrée dans un système d'information est l'humain. En effet, 95% des violations proviennent de l'erreur humaine (Findstack, 2022). *« Le réseau informatique peut être à la pointe des technologies de protection, si l'un des employés de l'entreprise n'est pas vigilant et clique sur un contenu piégé, l'entreprise sera touchée »*, **explique Arthur Bataille, CEO de Proph3cy**. *« Plusieurs techniques plus ou moins sophistiquées sont utilisées par les hackers pour exploiter la faille sécuritaire humaine, la plus courante étant le phishing. Depuis 2022, nous assistons également à une augmentation des attaques par smishing »*. Une tendance notamment portée par le développement du travail à distance.

Moindre protection des endpoints

En 2022, les attaques les plus sérieuses se sont portées sur les endpoints (terminal qui peut être connecté à un réseau comprenant des ordinateurs de bureau, des ordinateurs portables, des téléphones mobiles, des tablettes et des serveurs), les identités et les clouds. *« L'essor des Raas (Ransomware as a service) et la professionnalisation des hackers a affaibli les protections des endpoints»*, **explique François Berjamin-Salaun, Directeur Général chez Silicom & Open Cyber**. *« Des groupes créent des ransomwares et louent leur utilisation à des groupes spécialisés dans l'effraction virtuelle. La combinaison des deux spécialités rend les attaques beaucoup plus efficaces »*.

Développement du Cloud

Si les serveurs d'entreprise constituent le principal point d'entrée des pirates, le nombre d'intrusions signalées via le Cloud a considérablement progressé. Ainsi, selon l'étude OpinionWay pour le CESIN, la non maitrise de la chaine de sous-traitance de l'hébergeur (48%) et les difficultés de contrôles des accès par les administrateurs de l'hébergeur (43%) sont les deux principaux facteurs de risques émis par les entreprises en ce qui concerne l'utilisation du Cloud.

Fragilité de la chaine d'approvisionnement

En 2022, les attaques par la chaine d'approvisionnement ont pour leur part connu une augmentation de 650 % par rapport à 2021 (Rapport de la Sécurité 2022). Ce type d'attaque exploite les relations de confiance qui existent entre différentes organisations et cible le maillon le plus faible de cette chaine. Une fois qu'ils ont réussi à pénétrer dans le réseau de ce fournisseur, les attaquants peuvent alors accéder au réseau plus sûr par le biais de ce lien.

Augmentation de la surface d'attaque

D'autre part, la surface d'attaque des entreprises s'élargit du fait du travail à distance, de l'adoption généralisée de l'IoT (Internet des Objets) et du nombre important d'identités numériques créé pour une seule et même entreprise. Une augmentation de la surface qui fait également la part belle aux attaques basées sur la compromission et/ou usurpation des identités.

LEXIQUE

Le malware est un terme générique utilisé pour désigner une variété de logiciels hostiles ou intrusifs : virus informatiques, vers, cheval de Troie, ransomware, spyware, adware, scareware, etc. Il peut prendre la forme de codes exécutables, de scripts, de contenu actif et d'autres logiciels.

Le phishing est une technique frauduleuse destinée à leurrer les internautes en se faisant passer pour un organisme ou une personne de confiance afin d'entrer dans un système d'information et/ou récupérer des données sensibles de la victime. Il envoie un mail demandant généralement de «mettre à jour» ou de «confirmer» des informations suite à un incident technique (coordonnées bancaires, numéro de compte, codes personnels, etc.). Le phishing se décline en fonction des besoins des attaquants : le spearphishing nécessite par exemple une phase de reconnaissance plus importante, mais permet d'être plus efficace ; le smishing est une technique d'hameçonnage passant par les téléphones portables.

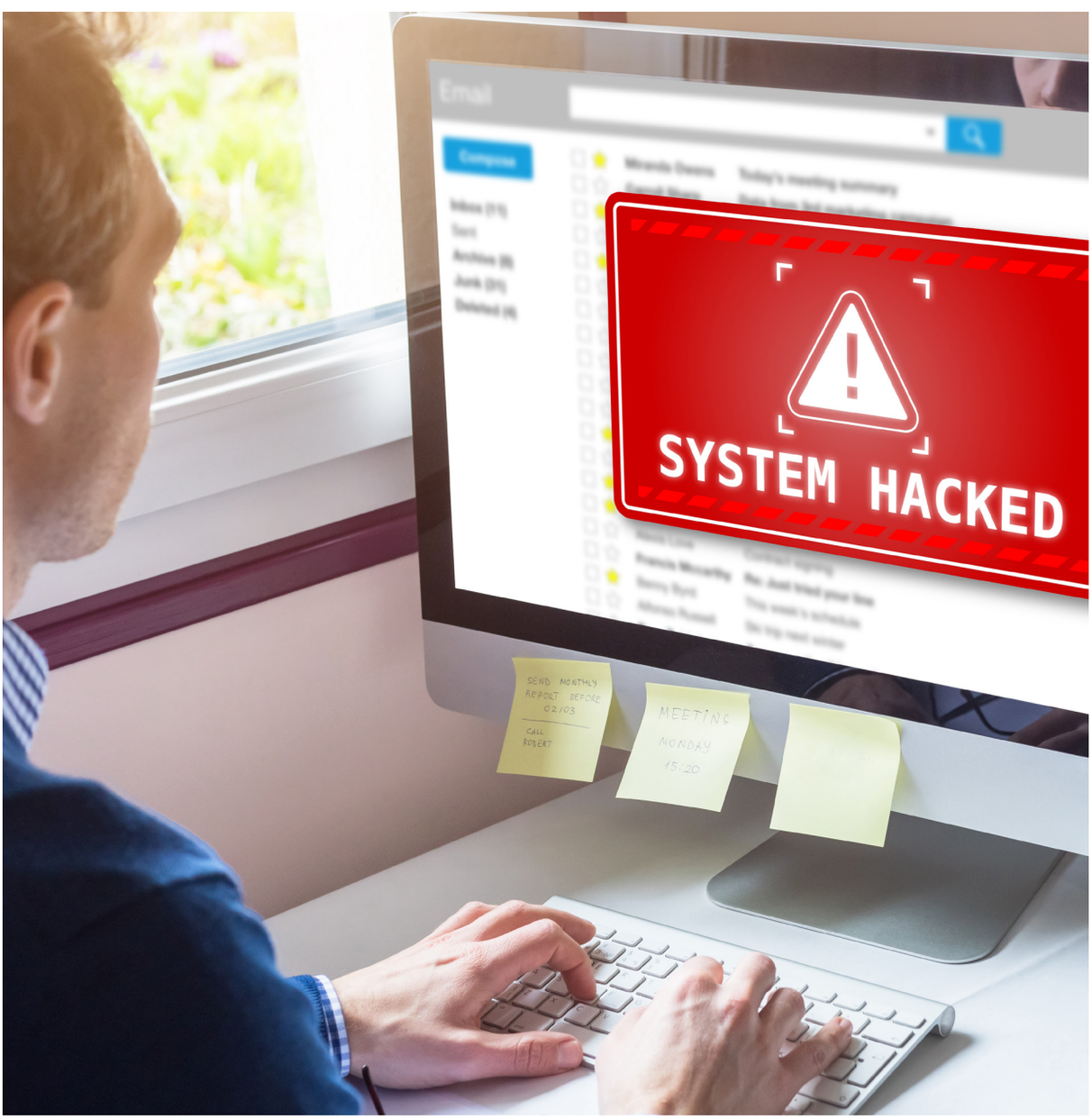
Le Ddos, Déni de service, vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé.

Les attaques man-in-middle : consistent à intercepter une conversation ou un transfert de données existant, soit en écoutant, soit en se faisant passer pour un participant légitime.

Les failles zéro-day, également orthographiée 0-day — ou faille / vulnérabilité du jour zéro est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. L'existence d'une telle faille sur un produit informatique implique qu'aucune protection n'existe, qu'elle soit palliative ou définitive

E | Conséquences de ces attaques

Les conséquences d'une attaque cyber peuvent être de différentes natures. Six entreprises sur dix ayant vécu une attaque ont ainsi été impactées sur leur business, principalement en raison d'une perturbation de la production (21%) ou par la compromission d'information (14%) (OpinioWay/CESIN). Deux entreprises sur cinq (41%) attaquées ont subi un détournement de paiement et parmi les entreprises françaises attaquées, 24% déclarent que leur solvabilité a été menacée (Rapport Hiscox 2022). *« Une entreprise sur deux qui ne paie pas la rançon réclamée par le cyber attaquant dépose le bilan dans les 18 mois suivant l'attaque »*, **rappelle ainsi Michel Van Den Berghe, Président de Campus Cyber**. Les pertes financières peuvent donc être directes ou indirectes. Les pertes directes sont dues au règlement de rançon et/ou d'amende à la suite de l'attaque, aux coûts liés à l'arrêt de l'exploitation et la gestion de crise, ou encore aux éventuels frais de notification de pertes de données…. Les pertes indirectes sont notamment liées aux conséquences de l'attaque cyber sur d'autres acteurs en raison des effets de contagions aggravés par les interdépendances numériques. *« Il convient également de ne pas négliger l'impact de ces attaques sur la réputation de l'entreprise,»* **poursuit Arthur Bataille CEO de Proph3cy.** *« Même si ce n'est généralement pas l'objectif recherché par les cyberattaquants, il représente un risque important pour l'entreprise victime ».*



2 SE PROTÉGER CONTRE LE RISQUE CYBER

Au sein même des entreprises, différentes mesures sont à mettre en place pour prévenir autant que possible les cyberattaques. De différentes natures, ces dispositifs vont du simple « bon sens » à des outils sophistiqués, en passant par la formation, les assurances, et la mise en place de process. L'intensité de ces mesures dépend alors de l'exposition et de la sensibilité au risque des entreprises.

A | Prévenir le risque

Sensibiliser les collaborateurs

L'humain est le principal point d'entrée des cyberattaques. La prévention de ce risque passe donc nécessairement en premier lieu par la sensibilisation et la formation de l'ensemble des collaborateurs de l'entreprise. *« Cette sensibilisation de tous les collaborateurs, y compris ceux réalisant des activités sans lien avec le cyber, est même indispensable pour que l'ensemble des autres mesures de protection mises en place par l'entreprise fonctionne,»* **explique Yasmine Douadi, Directrice stratégie cybersécurité de Seela et Proph3cy**. *« A partir du moment où l'employé a un accès ne serait-ce qu'à une toute petite partie du réseau de l'entreprise (comme une messagerie) alors il représente un potentiel point d'entrée pour une cyberattaque »*. Indispensable, cette sensibilisation des collaborateurs a d'ailleurs progressé depuis la crise sanitaire et le développement du télétravail. Selon l'enquête OpinionWay pour le CESIN, les mesures de sensibilisation au risque cyber des personnes en télétravail ont ainsi été renforcées pour 70% des entreprises interrogées.

« Cette sensibilisation passe en premier lieu par la diffusion d'informations auprès des collaborateurs, notamment sur les bonnes pratiques à adopter lorsqu'ils se connectent à Internet, ou pour protéger et sauvegarder ses données les plus sensibles,» **souligne Michel Van Den Berghe, Président de Campus Cyber**. *« Souvent, c'est une question de bon sens »*. Dans le cadre de cette démarche, les entreprises peuvent notamment se faire accompagner par le site Cybermalveillance.gouv.fr. *« Nous mettons à la disposition de nos publics de nombreux outils de sensibilisation tels que des guides, des kits, des vidéos pour les aider, à mieux comprendre et à faire face aux menaces»* **explique Jérôme Notin, Directeur général du GIP ACYMA cybermalveillance.gouv.fr**. *« Ces outils sont tous disponibles en licence Etablab2.0, de façon à ce que les organisations puissent s'approprier nos contenus et les personnaliser, afin de sensibiliser à leur tour leurs parties prenantes, être conscientes des risques encourus et sécuriser leurs équipements, tout en maîtrisant les réflexes et bonnes pratiques à adopter en matière de cybersécurité. »* Dans le cadre de cette sensibilisation, il convient également que l'entreprise réalise une veille régulière sur les différentes failles et techniques utilisées par les pirates afin de parer à toute éventualité d'attaque et construire ainsi une stratégie de sécurité la mieux adaptée aux enjeux du moment.

Assurer le risque cyber

L'assurance a également un rôle majeur à jouer dans la prévention et la prise en charge de ce risque. Elle permet aux différents acteurs de mieux l'anticiper et y répondre. En France, de nombreux assureurs du marché des risques d'entreprise proposent désormais une offre cyber. Ces garanties peuvent être intégrées dans des contrats classiques ou faire l'objet de contrats spécifiques. Dans le cadre de ces assurances, il convient néanmoins de veiller aux « exclusions » liées au risque cyber. *« Dans les assurances contre le risque cyber, il est recommandé de choisir un prestataire qui adapte le montant de sa prime à la totalité du risque auquel l'entreprise est exposée et qui n'exclut pas le remboursement de certaines prestations comme le coût de la remédiation et de la perte d'exploitation »*, **précise Jérôme Notin, Directeur général du GIP ACYMA cybermalveillance.gouv.fr.**

Questions à Jean Noël Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunications

En quoi l'indemnisation des rançons et cyberattaques par les assureurs permet-elle de lutter efficacement contre le risque cyber ? N'y a-t-il pas un risque que ces assurances soient contre-productives ?

« La doctrine de l'Etat pour les sites publics est toujours la même : nous ne payons pas les rançons demandées par les cybercriminels et nous recommandons aux entreprises de ne pas le faire.

Par ailleurs, les entreprises doivent mieux se préparer au risque cyber et être accompagnées par des experts mais aussi par d'autres acteurs de proximité, dont les assureurs. En cas d'attaque, pouvoir compter sur une assistance fournie par l'assurance et voir ses frais de reconstruction du système informatique pris en charge par l'assurance peut être utile.

Nous ne laissons pas de côté la prévention qui est la clé pour lutter contre ce risque. Les assureurs ont leur rôle à jouer en sensibilisant leurs assurés, et notamment les PME.

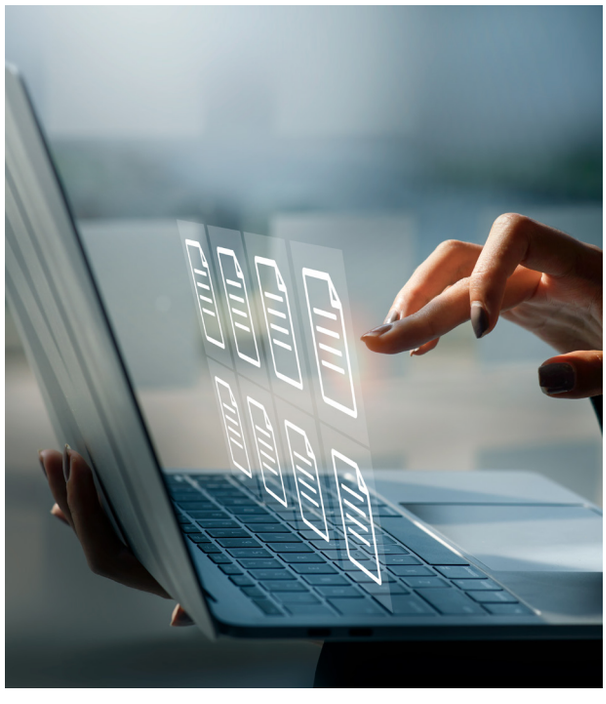
La démarche de l'Etat est avant tout d'augmenter l'information et la prévention. Il s'agit donc surtout de renforcer les moyens à disposition des entreprises, en particulier les plus petites, qui, si elles ne sont pas protégées, peuvent voir leur activité anéantie.

Les assureurs sont un relais utile dans le cadre de cette démarche de sensibilisation. En effet, ils entretiennent un dialogue régulier avec les assurés sur la nature des risques couverts et peuvent devenir acteur de cette prévention nécessaire. »

B | Repenser les process de gestion des risques

La cartographie des risques cybers auxquels l'entreprise peut être exposée et qui diffèrent en fonction de sa taille et se son secteur d'activité est indispensable à l'entreprise pour ensuite mettre en place les bons process de gestion de crise ainsi que les bons outils de sécurisation de son système d'information. Dans le cadre de cette démarche, l'entreprise doit se pencher sur la criticité de ses données, mais également sur l'organisation de ses ressources humaines et de son écosystème

- **Identifier les données les plus critiques :** Certaines données doivent être impérativement protégées d'une attaque pour ne pas mettre en danger l'entreprise. « *Tout l'enjeu pour les entreprises consiste à trouver le juste équilibre entre l'intérêt qu'elle représente et les risques qu'elle peut prendre* » **précise Alain Juillet, Président d'Honneur de l'Académie de l'Intelligence Economique**. « *Il faut préserver ce qui est essentiel sans pour autant bloquer tous les échanges et le travail collaboratif.* » Dans le cadre de cette analyse, il convient également que les entreprises prennent en considération le cycle de vie de leurs données.
- **Se pencher sur les droits d'accès des individus :** Cette démarche est valable pour les données, mais aussi pour les individus. Un collaborateur peut entrer dans une entreprise et évoluer de manière transverse dans différents départements, gravir différents échelons hiérarchiques ou encore être amené à quitter l'entreprise. « *Sa consommation des services numériques évoluera donc en conséquence*», **poursuit Nicolas Arpagian, Directeur de la Stratégie en cybersécurité de Trend Micro Europe, Enseignant à l'Ecole Nationale Supérieure de la Police et à Science Po Saint Germain en Laye**.» *Il convient de faire un suivi de qui a accès à quoi, pour faire quoi. Même si l'exercice est exigeant, c'est une condition d'une connaissance précise des usages numériques au sein de l'organisation. Cela facilite la détection des pratiques problématiques et la traçabilité des opérations* ».
- **Placer l'entreprise au cœur de son écosystème :** La prévention du risque cyber nécessite également de prendre en compte l'ensemble des partenaires, fournisseurs et sous-traitants de l'entreprise. « *Il faut toujours considérer l'entreprise comme étant partie prenante d'une chaine numérique au sein d'un écosystème, en gardant à l'esprit que les attaquants visent en priorité les éléments les plus faiblement protégés* », **ajoute Nicolas Arpagian.**



Nicolas Arpagian,
Directeur de la Stratégie en cybersécurité de Trend Micro Europe, Enseignant à l'Ecole Nationale Supérieure de la Police et à Science Po Saint Germain en Laye.

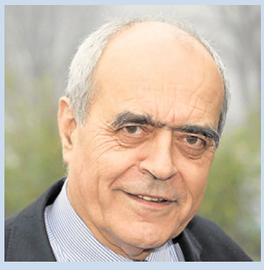
> Pour se protéger, il convient de combiner les règles juridiques avec la technologie. Dans le cadre de cette démarche, l'entreprise doit fixer des critères de protection et d'engagement avec des qualifications des données, des procédures de réponses à incidents, la mise en place de systèmes de sauvegarde et de gestion des accès. Il lui faut également avoir une vision qui soit la plus claire possible de toutes interactions techniques tant en interne que vers l'externe. Et veiller à toutes les évolutions pouvant les concerner. Il est primordial d'adapter les environnements techniques en fonction des données, des individus et des organisations connectées au système d'information. Cela conditionne l'instauration d'une politique de cybersécurité, qui devra être évaluée et sera adaptée en fonction des évolutions opérationnelles et de la réglementation.

85%

DES ENTREPRISES ESTIMENT QUE LES SOLUTIONS PRÉSENTES SUR LE MARCHÉ DE PROTECTION SONT ADAPTÉES À LEURS BESOINS

C | Mettre en place des solutions technologiques pour se protéger

La protection contre les cyberattaques passe également par la mise en place de solutions technologiques adaptées à l'exposition au risque de l'entreprise. Selon l'étude Opinion Way/CESIN, 85% des entreprises estiment d'ailleurs que les solutions présentes sur le marché sont adaptées à leur entreprise. Le nombre moyen de solutions mises en place dans les entreprises (plus de 10) reste élevé. En tête de ces solutions se trouvent notamment le VPN (91%) et le proxy (81). L'étude souligne également l'importante progression des solutions d'EDR (Endpoint detection and response) (68%, +17%) et de chiffrement (56%/+7%). En termes de détection des attaques, les entreprises tendent également à s'équiper de SOC (Security Operation Center).



Alain Juillet,
Président d'Honneur de l'Académie de l'Intelligence Economique

> Le choix de ces défenses techniques dépend de la situation de l'entreprise. En fonction de son degré de criticité, elle peut mettre en place des systèmes de mots de passe sur les ordinateurs pour créer une barrière au niveau de l'outil. Elle peut également mettre en place une sécurité plus globale à l'extérieur de l'entreprise, par exemple en implantant des systèmes de blocage des attaques s'articulant autour de l'intelligence artificielle, au niveau global dans les SOC ou sur les terminaux individuels tels que les systèmes d'EDR ou de XDR (Détection et réponses attendues)

LEXIQUE

LES PRINCIPAUX DISPOSITIFS DE PROTECTION ET DÉTECTION LES PLUS SOUVENT MIS EN PLACE DANS LES ENTREPRISES

VPN (réseau privé virtuel) : système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics (et en particulier Internet).

Proxy et filtrage d'URL : passerelle qui sert d'intermédiaire entre un ordinateur et les sites web et services Internet utilisés. Elle intercepte et gère le trafic entre deux appareils, réseaux ou protocoles.

Passerelle de sécurité mail : dispositif ou logiciel utilisé pour surveiller les courriers électroniques envoyés et reçus. Cet outil a pour vocation de se protéger contre les courriers électroniques indésirables (spam, phishing, logiciels malveillants ou frauduleux…) et de délivrer les bons courriers électroniques.

Authentification multi-facteur (MFA) : méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN

Solution et/ou service de scan de vulnérabilité : analyse complète qui détecte les vulnérabilités grâce à un processus entièrement automatisé basé sur des failles de sécurité connues.

Système de gestion des logs (SIEM) : logiciel qui identifie et catégorise les incidents et événements, et les analyse. Il fournit des rapports sur les incidents et événements liés à la sécurité, tels que les connexions réussies ou non, les activités malveillantes.

EDR (Endpoint Detection Response) : technologie logicielle de détection des menaces de sécurité informatique des équipements numériques (ordinateurs, serveurs, tablettes, objets connectés, etc.)

XDR (Extended Detection and Response) : surveille les Endpoints, mais aussi les emails, serveurs et le Cloud. En augmentant les capacités de détection, le XDR permet une réaction rapide aux menaces, en amont de la kill chain, limitant nettement les dégâts. Le XDR surveille en continu et de manière proactive pour alerter rapidement en cas de suspicion d'attaque.

SOC (Security Operation Center) : le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

3 MOBILISER ET FÉDÉRER AUTOUR DU RISQUE

Parallèlement aux différents dispositifs pouvant être mis en place dans les entreprises, la protection contre le risque cyber passe également par l'engagement et la mobilisation de tous, y compris l'état, autour de cet enjeu. Au-delà de la prise de conscience, il s'agit maintenant de fédérer les forces vives pour lutter efficacement contre le risque cyber.

A | La prise de conscience

Si de nombreuses actions peuvent être menées dans les entreprises, il convient néanmoins qu'elles soient pilotées par un véritable expert interne ou externe. C'est lui qui va nouer des liens et favoriser le partage des bonnes pratiques. *« Il faut créer de l'échange et instaurer une confiance entre les différents acteurs»*, **souligne Alain Juillet, Président d'Honneur de l'Académie de l'intelligence Economique.** *«Cela peut se faire au sein ou entre des clubs d'entreprises, des fédérations ou syndicats professionnels ou encore des associations. Ces différents liens doivent se construire et nous n'en sommes qu'aux balbutiements ». « Le gouvernement a un rôle de sensibilisation et d'information»*, **ajoute pour sa part Thibaut Lanxade Entrepreneur et Président-Directeur Général du Groupe Luminess**. *«Il lui revient notamment de renforcer la sécurisation des échanges, en légiférant (comme il l'a par exemple fait avec la réglementation à venir sur la facturation électronique obligatoire), en favorisant le Cloud Souverain ou encore en continuant d'investir dans la formation et la mise en place d'un écosystème pour lutter contre le risque cyber. »*

Une responsabilité dont convient d'ailleurs le gouvernement qui a initié plusieurs démarches en faveur de la lutte contre le risque cyber. *« La menace est réelle, se développe et surtout se standardise ce qui permet aux assaillants d'augmenter leur volume d'attaque,»* **déclare Jean-Noël Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunications**. *«Face à ce constat, les particuliers, les entreprises et les administrations doivent être mieux armés. C'est le sens des actions que je mène sous l'autorité de Bruno Lemaire, Ministre de l'Economie et des Finances, pour les soutenir et pour que chacun adopte les bons gestes barrières en ligne ».*

B | Les actions

Réguler

La cybersécurité occupe une place à part dans le domaine des technologies de l'information. *« Elle est toute à la fois façonnée par des enjeux techniques, économiques, juridiques et géopolitiques avec une implication des intérêts stratégiques des Etats,»* **précise Nicolas Arpagian, Directeur de la Stratégie en cybersécurité de Trend Micro Europe, Enseignant à l'Ecole Nationale Supérieure de la Police et Science Po Saint Germain en Laye.** *« Ainsi des pays comme la Chine, les Etats-Unis et même la Russie peuvent s'appuyer sur leur écosystème national respectifs avec des acteurs de référence (BATX, GAFAM, Yandex, VKontakte...), tandis que l'Europe est davantage en situation de consommatrice de services conçus et pilotés à partir d'autres continents que le sien. Cela explique l'importance prise par la production normative de l'UE, avec des textes structurants comme le Règlement Général sur la Protection des Données (RGPD) ou encore les directives NIS sur la protection des opérateurs de services essentiels (OSE), pour maîtriser au maximum le déploiement de politiques de cybersécurité.»*

Pour agir sur la cybersécurité et assurer un niveau de sécurité suffisant des acteurs économiques, plusieurs réglementations ont ainsi été mises en œuvre au niveau Français et/ou Européen tels que la Loi Godfrain du 5 janvier 1988, le Cybersecurity Act, le Règlement Général sur la Protection des Données (RGPD), la Norme ISO/CEI 27001, le Règlement DORA, la Directive NIS2 et plus récemment le Visa SecNumCloud.

Fédérer

Au-delà des réglementations, le gouvernement entend également mobiliser les différents acteurs de l'écosystème économique pour mieux lutter contre le risque cyber. Une démarche qui passe par l'impulsion, la mise en place et puis le soutient d'organisations propres à accompagner les entreprises et collectivités dans la prévention et la gestion du risque cyber, mais également à former et développer des expertises autour de ce sujet.

> L'ANSSI

L'état œuvre ainsi au travers de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. En qualité d'acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

> Cybermalveillance.gouv.fr

En 2017, l'ANSSI et le ministère de l'Intérieur ont créé Cybermalveillance.gouv.fr, le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de prévention et sensibilisation aux risques numériques et d'observation de la menace. « *Nous avons pour vocation d'accompagner les particuliers, les entreprises (hormis celles dont s'occupent l'ANSSI) et les collectivités territoriales* », **Jérôme Notin, Directeur Général du GIP ACYMA cybermalveillance.gouv.fr.**

La mission consiste à assister les victimes d'actes de cybermalveillance, en assurant un service d'assistance en ligne et une mise en relation avec des professionnels en sécurité numérique référencés sur la plateforme. Le groupement a également pour vocation de prévenir les risques et de sensibiliser aux bonnes pratiques en sécurité numérique, avec la production de différents contenus, et à travers l'accompagnement à la sécurisation des systèmes d'information des publics professionnels par des prestataires labellisés ExpertCyber. Enfin, cybermalveillance.gouv.fr a pour rôle d'observer le risque notamment au travers de ce que remontent les prestataires et les victimes afin d'adapter en conséquence le contenu de ses outils de prévention ainsi que ses parcours d'accompagnement à la lutte contre le risque cyber.

Ce dispositif piloté par une instance de coordination, le Groupement d'intérêt Public (GIP) ACYMA, est composé d'une soixantaine de membres issus du secteur public, du privé et du domaine associatif, et qui contribuent chacun à sa mission d'intérêt général. « Gage de l'intérêt de ce partenariat public/privé, en cas d'incident de cybersécurité majeure, nous diffusons par exemple une « Alerte Cyber » auprès de nos membres (parmi lesquels MEDEF, CPME ,U2P et AMF), qui la relaient à leurs adhérents, poursuit Jérôme Notin. Ce dispositif a été lancé en 2021 par le secrétaire d'Etat Cédric O en 2022 et touche un potentiel de 3,5 millions d'organisations

> Campus Cyber

Plus récemment en 2021, le Président de la République Emmanuel Macron a initié le projet de Campus Cyber, qui consiste à rassembler en un lieu « totem » l'ensemble des acteurs nationaux et internationaux liés à la cyber sécurité. Le Campus Cyber s'articule également autour de forces vives issues aussi bien du privé que du public. « *Ce Campus est aujourd'hui porté par des acteurs privés et soutenu par l'état (40% de l'actionnariat), et rassemble désormais plus de 250 entités qui représentent l'ensemble de l'écosystème : banques, transports, sociétés spécialisées dans le risque cyber, start-up, organismes de formation, acteurs de la recherche et des associations* », **précise Michel Van Den Berghe, Président du Campus Cyber.** « *Nous avons pour vocation de mettre en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs : partage de bonnes pratiques, création de projets opérationnels… Notre rôle consiste également à promouvoir l'excellence française en matière de cybersécurité, en centralisant les talents et les acteurs du secteur dans un lieu commun autour de projets d'innovations. Nous hébergeons à ce titre un incubateur de jeunes entrepreneurs qui souhaitent développer un projet autour du risque cyber. Nous entendons également participer à la formation d'expert en sécurité et cyber sécurité et créer de l'attractivité autour de ces métiers* ».

C | La souveraineté numérique, une solution ?

Les technologies numériques prennent une importance croissante dans les activités de production, de gestion, de commercialisation et d'administration des entités privées et publiques. La question de la souveraineté technologique comme composante de la sécurité collective s'invite également dans le débat de la lutte contre le risque cyber. *« Cependant, il reste encore difficile de parler de souveraineté numérique en France voir même de l'envisager car pour le moment la France n'a pas réalisé la globalité des investissements nécessaires à sa mise en place, notamment en termes de recherches et formation,»* **précise Alain Juillet Président d'Honneur de l'Académie de l'Intelligence Economique**. *Certaines technologies ou outils existent malgré tout et proposent les contours d'une souveraineté numérique partielle. C'est notamment le cas pour certaines solutions EDR ou XRD. De même, OVH travaille actuellement au développement d'un Cloud Souverain. Il faudrait néanmoins investir bien davantage»*. D'autre part, le principe de souveraineté numérique reste assez éloigné des préoccupations actuelles des entreprises qui jonglent au quotidien avec des problématiques commerciales, financières, fiscales, juridiques, sociales ou encore technologiques. *« C'est la raison pour laquelle les entreprises du privé lui préfèrent le principe d'autonomie, qui désigne la faculté d'agir librement,»* **précise Nicolas Arpagian**. *«Elles ont à cet effet besoin de comprendre le fonctionnement des technologies qu'elles achètent et ce qui est fait des données exploitées par ces applications ».*

Pour répondre à ce double enjeu et tendre vers la souveraineté numérique, il faudrait donc favoriser l'émergence de solutions technologiques propres à limiter autant que possible le risque cyber mais aussi le développement de compétences et d'expertises capables de concevoir ces technologies de lutte contre les cyberattaques et d'accompagner les entreprises en la matière. *« Il devient donc urgent de miser sur la formation, initiale et continue, pour élargir le nombre et l'origine des talents qui peuvent s'exercer dans le domaine de la cybersécurité,»* **poursuit Nicolas Arpagian.** *« Cette expertise est indispensable pour assurer la souveraineté à laquelle les démocraties aspirent ».*

Malgré ces différents dispositifs et investissement l'état ne peut et ne pourra pas tout. *« Il revient également aux éditeurs, consultants, conseillers et autres sociétés de service d'accompagner les entreprises,»* **conclut Thibault Lanxade, Entrepreneur et Président-Directeur Général du Groupe Luminess** *« Ce rôle de pédagogie et de sensibilisation des entreprises revient également aux Chambres de Commerce et d'Industrie et aux Chambres des métiers, aux organisations patronales, experts comptables, commissaires aux comptes et avocats ».*

Questions à Jean Noël Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunications

Quelle est la feuille de route du Gouvernement concernant la lutte contre le risque cyber ?

Face à la cybercriminalité qui évolue, je veux garantir la cybersécurité du quotidien. J'ai annoncé récemment, pour l'année 2023, une enveloppe de 30 millions d'euros pour des actions de sécurisation. Ces actions comprennent plusieurs volets qui couvrent tous les Français.

Pour les entreprises, nous allons réaliser une campagne massive de communication, en lien avec cybermalveillance.gouv.fr, pour inciter les entreprises à s'inscrire dans une démarche de cybersécurité. De plus, un outil d'auto diagnostic, gratuit, en ligne et de référence sera créé pour permettre à toutes les entreprises de connaitre leur niveau de protection et les premières mesures à mener. Enfin, pour 750 PME et ETI, issues des secteurs stratégiques visés par la directive NIS2, le Gouvernement mettra en place un bouclier cyber avec une phase d'évaluation et d'audit puis la mise en œuvre de solutions de sécurité.

Vous renforcez également vos actions aux côtés des collectivités ?

Pour les collectivités, nous prolongerons les parcours de cybersécurité en les renforçant pour 125 des 950 collectivités qui ont déjà bénéficié du plan 2021-2022 et en permettant à 50 nouvelles collectivités de commencer ce programme. En août 2022, j'avais annoncé, avec l'accord de la Première ministre, une enveloppe supplémentaire de 20 millions d'euros dédiée spécifiquement aux hôpitaux. Au total, fin 2023, ce sont plus de 1 000 collectivités et administrations qui auront suivi ce programme.

De plus, pour toutes les communes et y compris les plus petites, une plateforme de services mutualisés sera créée. Il s'agit d'un outil clé en main, sur la base d'un abonnement, via lequel l'État proposera notamment aux collectivités de bénéficier d'un nom de domaine, d'une messagerie et de services en ligne sécurisés.

Et pour les particuliers ?

Pour les particuliers, conformément à l'engagement du Président de la République, le filtre anti-arnaque sera mis en place en version bêta à l'été 2023 avant d'être généralisé à l'été 2024. Simple, facultatif et gratuit, il sera basé sur l'analyse de la menace cyber en temps réel et permettra d'avertir les internautes (web et mobile) en filtrant préventivement les adresses web malveillantes.

Enfin, nous développerons également le cyberscore. Fruit des travaux parlementaires, il certifiera les plateformes numériques destinées au grand public. Déployé d'ici la fin 2023, il permettra aux internautes d'avoir une idée générale du niveau de sécurité des sites qu'ils fréquentent en majorité, à l'image du Nutri-score pour les produits alimentaires.

CONCLUSION

Si les entreprises et collectivités commencent à mesurer les dangers des cyberattaques et que le gouvernement renforce ses dispositifs d'accompagnement, des efforts restent à faire pour lutter efficacement et durablement contre ce risque immatériel. Une démarche qui ne pourra se faire qu'en fédérant et en mobilisant le plus grand nombre autour de cet enjeu.

D'autre part, le meilleur bouclier contre ce fléau reste la connaissance et la maitrise des risques et des solutions propres à le prévenir voire à l'éradiquer. C'est la raison pour laquelle nombre d'intervenants à ce guide ont pointé l'urgence de former et de développer de nouvelles expertises pour favoriser la conception de stratégies et de solutions de cyber sécurité. Une démarche qui passera certes par des investissements mais aussi par l'innovation, que ce soit en termes de méthodes d'apprentissage ou de contenu des formations relatives à ce sujet.

Les professionnels de la sécurité, les universitaires et chercheurs, mais également l'état, les entreprises et les organismes et fédérations professionnelles doivent donc continuer à se mobiliser ensemble pour faire émerger les solutions et expertises nécessaires à la lutte contre le risque cyber.

L'ÉQUIPE DIRIGEANTE

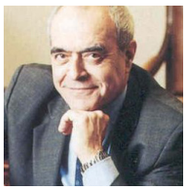
Charles BATTISTA
Président

Sébastien BOUCHINDHOMME
Délégué général

Paola FABIANI
Conseillère

MEMBRES D'HONNEUR

Sonia ARROUAS
Présidente du Tribunal de commerce d'Evry



Alain JUILLET
Président d'honneur de l'Académie de l'intelligence économique

Thibault LANXADE
Entrepreneur, Président de Luminess

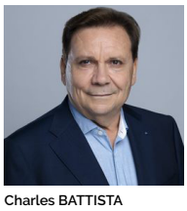
Corinne LEPAGE
Ancienne ministre de l'Environnement, ancienne eurodéputée et avocate associée fondatrice du cabinet Huglo Lepage Avocats

Jean-Claude MAILLY
Ancien Secrétaire général de Force Ouvrière

Michel SAPIN
Avocat, Ancien Ministre

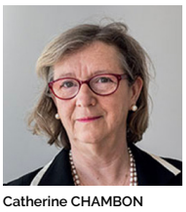
LE COMITÉ SCIENTIFIQUE

Jean-Luc BARAS
Président du Conseil National des Achats



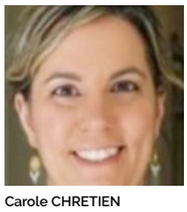
Charles BATTISTA
Président de la FIGEC

Philippe BERNA
Médiateur national délégué à la Médiation des entreprises

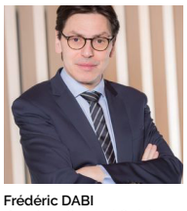


Catherine CHAMBON
Sous-directrice de la lutte contre la cybercriminalité au Ministère de l'intérieur

Jo-Michel DAHAN
Conseiller – Médiateur des entreprises

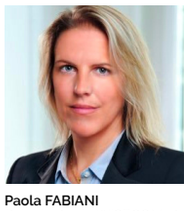


Carole CHRETIEN
Directrice relations entreprises CNRS



Frédéric DABI
Directeur Général Opinion IFOP

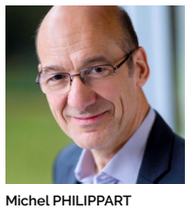
Michel DIETSCH
Professeur émérite à l'UNISTRA



Paola FABIANI
Présidente de WISECOM et du COMEX40 du MEDEF

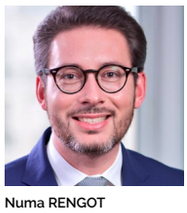
Denis FERRAND
Directeur Général de REXECODE

Jacky ISABELLO
Co-fondateur CorioLink



Michel PHILIPPART
Directeur général de Glion Institute of Higher Education

Louis-Rémy PINAULT
Expert développement stratégique chez GENERAL



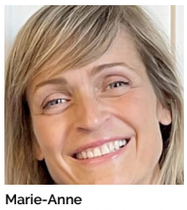
Numa RENGOT
Avocat associé Franklin

LE COMITÉ D'EXPERTS

Sofiane ABOUBEKER
Président d'ARECIA

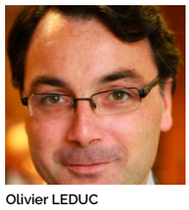
Anthony BENHAMOU
Economiste – Enseignant à Sciences Po Paris

Valentin CLEMENT
Etudiant EDHEC



Marie-Anne DESNOULEZ-DELDIQUE
Co-fondateur WeTalk Group

David GRUSON
Directeur Programme Santé Jouve / Fondateur ETHIK-IA

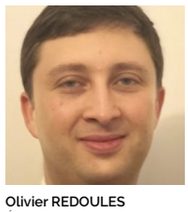


Olivier LEDUC
Expert-comptable

Frédéric LEFRET
Président de l'Institut du Dialogue Civil

Philippe LOREC
Chargé de mission au Service du Haut Fonctionnaire de Défense et de Sécurité

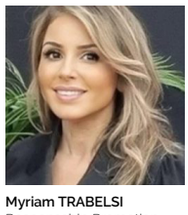
Virginie MARTIN
Professeure à Kedge, Politiste, sociologue



Olivier REDOULES
Économiste

Stéphanie VERILHAC-MARZIN
SVM Consult

Mélanie PERCHERON
Arbitre international de judo



Myriam TRABELSI
Responsable Promotion économique – Grand Paris Grand Est

Etymologiquement le lieu des « échanges » – Place Escange est l'endroit privilégié, regroupant acteurs publics et acteurs privés, pour mener une réflexion prospective sur la prise en compte et l'évolution du capital immatériel des entreprises.

Place Escange est soutenu par la Fédération Nationale de l'Information d'Entreprise, de la Gestion de Créances et de l'Enquête Civile.

www.place-escange.fr

@PlaceEscange

@place-escange

Contact : sbouchindhomme@figec.com