...LA CYBERSÉCURITÉ DES ENTREPRISES. PRÉVENIR ET GUÉRIR : QUELS REMÈDES CONTRE LES CYBER VIRUS ?

1. UN ENJEU DÉCISIF DE SURVIE DES ENTREPRISES

La cybercriminalité visant les entreprises se banalise pour quatre motifs :

1. **La numérisation de l'économie, accélérée avec le confinement lié au développement du télétravail et au déploiement de la fibre ;**
2. **La professionnalisation de la cybercriminalité,** facilitée par sa **« plateformisation », son industrialisation, et le développement des cryptomonnaies ;**
3. **La difficulté de la prévention et de la répression**, lesquelles nécessitent à la fois la prise de conscience de tous et une coopération internationale efficiente ;
4. **L'intégration du cyberespace comme nouveau vecteur de la conflictualité géopolitique** dont les entreprises sont soit les cibles soit les victimes collatérales.

Or, l'économie numérique, et tout particulièrement le e-commerce, ne peuvent se développer qu'en se fondant sur **la confiance des partenaires de l'entreprise et des consommateurs.**
Les entreprises, quelle que soit leur taille, sont **incitées à numériser** leurs processus de production, à développer le e-commerce, à placer leurs salariés en télétravail. Les entreprises les plus petites pensent être **à l'abri** des cyberattaques. C'est **une illusion, parfois mortelle** : une entreprise peut fermer après une cyberattaque. Les coûts indirects se révèlent parfois avec un fort délai de latence.

Chaque utilisateur d'un outil numérique ou même d'un objet connecté **peut-être potentiellement le maillon faible du filet de cybersécurité tendu dans la Toile. L'explosion des usages numériques s'est accompagnée d'une hausse exponentielle des actes de piratage.** Quelques chiffres suffisent à illustrer ce phénomène :

6 000	*milliards de dollars par an à partir de 2021, contre 3 000 milliards en 2015 , tous secteurs confondus, tel est le coût de la cybercriminalité au niveau mondial*
3ème	*économie mondiale si le cyberrisque était un pays*
43 %	*des PME ont constaté un incident de cybersécurité en 2020*
16 %	*des cyberattaques menacent la survie d'une entreprise en 2020*
+ 155 %	*de fréquentation du site cybermalveillance.gouv.fr en 2020*
X 4	*des attaques au rancongiciel entre 2020 et 2021 selon l'ANSSI*

Le président de la Réserve fédérale des États-Unis, Jerome Powell, considère que les cyberattaques contre les entreprises constituent le **risque actuel le plus important pour l'économie américaine, plus redoutable encore qu'une crise financière similaire à celle de 2008.** Face à cette internationalisation du cybercrime, le Président de la République française a présenté le 12 novembre 2020, au Forum sur la gouvernance d'Internet, un **« *appel de Paris* » pour la sécurité du cyberespace.**

2. UNE PRISE DE CONSCIENCE TARDIVE ET INSUFFISANTE DE L'AMPLEUR DES CYBERMENACES

La cybersécurité était, en 2018, loin d'être considérée comme « *l'affaire de tous* », comme le déplorait CCI France. De trop nombreuses entreprises, notamment les PME et TPE, ne se sentaient pas concernées. Le sujet semblait technique, externalisable, solutionnable par le simple achat d'un pare-feu !

Cependant, un basculement s'est opéré au printemps 2020. La surface d'exposition aux cyberattaques a été nettement augmentée avec plus de 8 millions de salariés en télétravail. Dans un premier temps, de nombreuses entreprises ont même encouragé leurs salariés à utiliser leur propre équipement informatique. Cette situation a créé des brèches de sécurité, l'urgence étant la continuité de l'activité davantage que la sécurité numérique. Les cybercriminels en ont profité, avec une **augmentation de 667 % des attaques par *phishing* enregistrées entre le 1er et le 23 mars 2020**.

Les dirigeants d'entreprise intègrent désormais ce risque de façon croissante, bien qu'inégale.

Face à la montée des failles de sécurité, leurs services informatiques tentent désormais d'imposer le **concept Zero Trust**, modèle de sécurité qui repose sur le principe qu'aucun utilisateur n'est totalement digne de confiance sur un réseau.

Cette nécessité est prise en compte par les grandes entreprises, d'autant que **les agences de notation intègrent le risque cyber dans leur notation financière** et qu'un marché de la notation cyber s'est développé. En outre, **la notation ESG** (environnement, société, gouvernance) comporte également une référence à **la cybersécurité.** Elle constitue une **dimension essentielle de la gouvernance de l'entreprise** mais également de **la responsabilité sociétale** des entreprises sous l'angle de la protection contre le vol des données. La Plateforme RSE préconise même de créer une « responsabilité numérique des entreprises » (RNE).

Le niveau de cybersécurité des entreprises doit être **rapidement et fortement augmenté avant l'explosion de l'internet des objets** (IoT), qui va étendre de façon exponentielle la surface d'exposition au cyberrisque, **de l'ordinateur quantique** qui démultipliera les capacités d'intrusion, ou encore de **l'Intelligence Artificielle**.

3. UN DISPOSITIF DE CYBERPROTECTION PUBLIQUE PRIVILÉGIANT LES ENTREPRISES D'IMPORTANCE VITALE

Les entreprises qualifiées d'**opérateurs d'importance vitale (OIV)** sont protégées de manière satisfaisante à l'échelle européenne et nationale, par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). En revanche, les TPE et PME, comme celles des ETI qui ne sont **pas** identifiées comme **d'importance vitale, ne sont pas assez bien cyberprotégées** par ce dispositif public.

La cybersécurité publique se caractérise par un **équilibre entre centralité de la compétence technique et proximité** des victimes potentielles avec la possibilité de déposer plainte dans les gendarmeries et commissariats**.**

Elle assure une **répartition originale des compétences non en fonction de la localisation de l'infraction (critère territorial) mais en fonction de la famille de rançongiciel à traiter (critère fonctionnel).** La taille de l'entreprise est neutre dans le traitement judiciaire de la cyberattaque.

Ce dispositif public comprend **une capacité de projection de forces d'intervention sur le terrain à même de rassurer un dirigeant d'entreprise,** lequel, le plus souvent, ignore les compétences numériques de la Police nationale ou de la Gendarmerie.

La cybersécurité des entreprises **repose sur le bon fonctionnement d'une quadruple coopération** afin de partager l'information à des fins de prévention, de remédiation et de sanction :

- entre les autorités judiciaires et les forces de cybersécurité,
- entre la police et la gendarmerie, qui se sont chacun dotés d'outils distincts,
- entre le secteur public et les acteurs privés,
- entre la France et ses partenaires européens, et même internationaux.

Toutefois, **la justice reste démunie alors que le cybercrime s'est industrialisé**.

4. UNE CYBERSÉCURITÉ DIFFICILEMENT ACCESSIBLE AUX PME

Des grandes entreprises mieux protégées, des PME plus vulnérables

Les cybercriminels font des études de marché sur leurs cibles. Lorsque celles-ci ont atteint un niveau supérieur de protection, ils réorientent des attaques sophistiquées via leurs fournisseurs ou sous-traitants plus fragiles en termes de cybersécurité. Face à la multiplication des cyberattaques, **les grandes entreprises et les ETI ont pris des mesures de défense compliquant la tâche des cybercriminels**. En particulier, les stratégies de sauvegarde et de reconstruction efficace des systèmes informatiques rendent le blocage des systèmes moins pertinent comme contrepartie à une demande de rançon. **Une meilleure cyberdéfense des grandes entreprises a eu comme contrepartie de détourner la cybercriminalité vers les plus petites entreprises plus vulnérables.** Cette translation du risque vers des fournisseurs, sous-traitants ou clients, continue cependant à affaiblir, par rétroaction, la cybersécurité des grandes entreprises. En effet, l'accès à distance au système d'information de l'entreprise augmente sa surface d'attaque en ouvrant de nouvelles portes.

« L'effet domino » peut être dévastateur. La cybersécurité est donc l'affaire de tous et de toute la chaine de valeur.

Le salarié est souvent le maillon faible de la cybersécurité, voire un « cheval de Troie ».

La cybersécurité est encore trop perçue comme **une contrainte supplémentaire** par les salariés eux-mêmes. L**e fonctionnement en silos** du management d'un certain nombre d'entreprises ne favorise pas toujours ce travail d'équipe. Une collaboration minimaliste ne permet pas de diffuser de façon efficace une culture partagée. Celle-ci doit impliquer tous les échelons de la hiérarchie de l'entreprise, en intégrant les dirigeants et l'ensemble du management, leur rôle d'impulsion étant majeur.

La lutte contre les cybervirus suppose une **hygiène numérique constante** et des « **gestes barrières »** permanents de la part de chacun. L'augmentation du budget alloué aux outils n'est pas une réponse suffisante face à la multiplication des menaces de plus en plus sophistiquées. **Chaque salarié dispose de la clé de la cybersécurité de son entreprise.**

La pénurie d'expertise humaine en matière de cybersécurité est mondiale. Dès lors, **ce handicap est particulièrement aggravé pour les TPE - PME** pour lesquelles la ressource humaine devient pratiquement inaccessible. Au déficit de compétences en cybersécurité s'ajoute

le fait que les entreprises **ne mesurent pas à sa juste valeur l'intérêt de sécuriser l'information.**

Un recours croissant au cloud dans une relation commerciale déséquilibrée

Pour **accéder au cloud**, les PME sont dans une situation inconfortable. Elles n'en maîtrisent pas techniquement les enjeux et souffrent **d'une relation commerciale déséquilibrée**. Certains fournisseurs déclinent même toute responsabilité en matière de disponibilité ou de fonctionnalité du service.
Malgré le principe de libre circulation des données, traduite par le règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018, et les lignes directrices du 29 mai 2019, **le processus d'autorégulation du marché du cloud s'est interrompu** en novembre 2019, faute d'accord sur la rédaction de codes de conduite.
Il existe une **asymétrie systémique entre grands fournisseurs mondiaux de services cloud et leurs utilisateurs.** Pour une PME, accéder au cloud s'apparente parfois à conclure un contrat d'adhésion pouvant contenir des clauses parfois abusives.

5. LE SURSAUT OU LE CHAOS : L'URGENTE CONSOLIDATION DE L'ÉCOSYSTÈME FRANÇAIS DE LA CYBERSÉCURITÉ

Un objectif ambitieux de leadership en matière de cybersécurité

Si la cybersécurité est une menace pour les entreprises, elle constitue également une **opportunité de développer un marché porteur.** Elle représente en France **13 milliards d'euros de chiffre d'affaires.** Ce secteur est en forte croissance. Il dégage 6,1 milliards d'euros de valeur ajoutée et emploie 67 000 personnes. Le marché mondial de la cybersécurité devrait représenter **150 milliards de dollars en 2023.**
L'offre française de cybersécurité demeure **très fragmentée** avec une **forte exposition à la concurrence** mondiale. Notre pays comporte toutefois des leaders mondiaux. Il dispose **d'atouts** de premier plan pour pérenniser son **avance technologique et économique**, notamment dans trois domaines : l**'Intelligence Artificielle** et l'apprentissage automatique (le ***machine learning*****),** la **cryptographie** et la **technologie post-quantique.**
Associée jusqu'ici à l'idée de contraintes et de dépenses, la cybersécurité doit être considérée aujourd'hui comme un atout compétitif et un investissement productif. Un comportement cybersécurisé devient un critère de sélection pour les clients soucieux à l'idée de confier des données personnelles, voire sensibles, à une entreprise.

La **stratégie de l'État** vise à encourager le développement d'un **écosystème** de la cybersécurité.
La cybersécurité et la sécurité de l'Internet des Objets (IoT) est l'une des cinq priorités du contrat stratégique de la filière « industries de sécurité » du 29 janvier 2020, avec la sécurité des grands évènements et des Jeux Olympiques de Paris 2024, l'identité numérique, les territoires de confiance et le numérique de confiance. Il s'agit de *« positionner l'industrie française comme* ***leader mondial*** *de la cybersécurité et de la sécurité de l'IoT* ». **L'objectif est ambitieux.**

Le développement de l'excellence de la filière française de cybersécurité devrait davantage se traduire par une politique publique d'achat de solutions de cybersécurité françaises. Ce n'est hélas pas le cas. L'achat de solutions étrangères non maîtrisées est susceptible de menacer la souveraineté de la France. Il manque une culture d'achat de produits français de cybersécurité.

Afin de **fédérer la communauté** de la cybersécurité, un **cybercampus** doit s'installer à l'automne 2021 à la Défense. Ce « *lieu totem de la cybersécurité* » doit rassembler les principaux acteurs nationaux, publics et privés, et les inciter à développer des **synergies**. Il est indispensable qu'il incarne le sursaut de la France face au volume exponentiel des cyberattaques qui menacent toutes les organisations, tant privées que publiques. **A défaut de sursaut, nous risquons le chaos à brève échéance !**

Une impossible reconquête de la souveraineté numérique dans le cloud

Le marché du cloud devrait exploser en passant de 63 milliards d'euros en 2021 à 560 milliards en 2030. La maîtrise des données des entreprises est un enjeu de souveraineté. Il est difficile à la France de **recouvrer sa souveraineté dans le cloud**, dominé actuellement par **trois acteurs américains qui possèdent 70 % de parts de marché.** Il s'agit pourtant du **socle incontournable du développement des entreprises, y compris des PME,** comme celles des entités publiques, soumises aux mêmes menaces.

La volonté de retrouver la souveraineté des données est régulièrement évoquée en France depuis 2010. Après **l'échec d'Andromède**, l'État français rejoint en mai 2020 l'initiative allemande **Gaia-X** et abandonne l'idée de créer *ex-nihilo* une nouvelle entreprise soutenue par la puissance publique et de grandes entreprises. L'objectif est désormais de former une infrastructure européenne articulée autour d'un organisme de gouvernance et de coordination chargé d'émettre des standards de sécurité, d'interopérabilité et de portabilité des données.
La stratégie nationale pour le cloud de mai 2021 acte l'avance non rattrapable du **secteur privé américain**. Il s'agit désormais de **maîtriser notre dépendance dans la durée**. Le pari gouvernemental invoque le précédent du nucléaire, notre autonomie s'étant développée sous licence de technologies américaines.

6. METTRE LA CYBERSÉCURITÉ À LA PORTÉE DE TOUTES LES ENTREPRISES

L'adage « *mieux vaut prévenir que guérir* » s'applique tout particulièrement à la cybersécurité. La réalité oblige à traiter ces deux volets. S'y ajoute la nécessaire sanction des cybercriminels.

Le rapport propose <u>trois axes de propositions</u> pour développer le cercle vertueux de la cyberprotection : tester, alerter, protéger.

AXE 1 : TESTER ET RENFORCER LA RÉSISTANCE ET LA CYBERRÉSILIENCE DES ENTREPRISES

Le dispositif ***cybermalveillance.gouv.fr*** doit être mieux promu auprès des entreprises et un service d'urgence doit être dédié aux entreprises, en mobilisant des **jeunes** en service civique et disposant des compétences numériques adéquates **(proposition n°1)**.

Un **recueil anonymisé des plaintes** doit être ouvert afin d'encourager les entreprises à signaler les cyberattaques sans porter atteinte à leur réputation, tout en décourageant la publicité autour des logiciels malveillants, afin de disposer de statistiques fiables **(proposition n°2).**

Des équipes de réponse aux incidents informatiques (CSIRT : *Computer Security Incident Response Team*) doivent être déployées **dans les Régions,** afin de faciliter l'accès des PME à la cyberprotection tout en **sensibilisant les collectivités locales**. Ces dernières sont, avec les hôpitaux publics, les **nouvelles cibles de la cybercriminalité (proposition n°3).**

Pour renforcer la résistance du tissu entrepreneurial, l'État doit :

- élaborer **des plans nationaux de prévention des cyberrisques** ;
- **coordonner les réponses** des pouvoirs publics et des acteurs privés **en cas d'attaque numérique systémique,** affectant une part significative des entreprises quelle que soit leur taille,
- et organiser régulièrement des **exercices de simulation** (proposition n°5).

AXE 2 : ALERTER, CONSEILLER, FORMER SUR LE PÉRIL CYBER

Salariés et dirigeants d'entreprise doivent être davantage sensibilisés à la cybersécurité, à l'hygiène numérique et ses gestes barrières :

- Les salariés, en se voyant proposer une **sensibilisation à la cybersécurité par la voie de la formation professionnelle** (**proposition n°9**).
- Les **dirigeants**, dont la responsabilité personnelle peut être engagée en cas de cyberattaque de la chaîne de valeur dont ils sont partie prenante, en étant mieux sensibilisés du risque de devenir à la fois être victime et responsable. Le sujet doit être traité lors de la définition de la stratégie de l'entreprise (**proposition n°15**).

La certification par un **référentiel de cybersécurité** accessible aux PME et TPE doit être encouragée (**proposition n°14**).

Afin de souligner la nécessité de renforcer la **conception sécurisée** (*security by design)*, la « garantie logicielle », concernant les mises à jour de sécurité, doit être étendue aux entreprises ; et un **hackathon de la cybersécurité des entreprises** pourrait être organisé avec le support de l'ANSSI, ciblant notamment les logiciels mis sur le marché, chaque 30 novembre, Journée mondiale de la cybersécurité (**proposition n°13**).

Afin de sensibiliser le grand public à la cybersécurité, un **cyberscore des plateformes numériques** doit être instauré, comme le Sénat l'a récemment proposé (**proposition n°22**), et une **campagne massive de promotion des métiers** de la cybersécurité doit être déployée (**proposition n°10**).

AXE 3 : PROTÉGER LES ETI, PME ET TPE PAR DES OUTILS ADAPTÉS

Le dispositif public de cyberprotection doit être renforcé en moyens humains et financiers.

La création d'un **cybercampus** fédérant les acteurs publics et privés de la cybersécurité constituera un atout dans la lutte contre la cybercriminalité.

Pour renforcer la réponse pénale à la cybercriminalité, il faut développer la formation initiale et continue des magistrats en matière de cybercriminalité ; augmenter les effectifs spécialisés en cybersécurité des forces de sécurité ; doter les forces de cybersécurité de moyens financiers adéquats ; étudier la faisabilité de la création d'un Parquet national de lutte contre le cybercrime ; et créer, à chaque degré de juridiction, une chambre spécialisée dans la lutte contre la cybercriminalité (**proposition n°6**).

Pour répondre à l'industrialisation de la cybercriminalité, **les procédures pénales doivent être adaptées pour accélérer la réponse judiciaire et renforcer la coopération** avec l'ANSSI au-delà de la lutte contre le terrorisme (**proposition n°7**).

La présidence française de l'Union européenne au premier semestre 2022 doit être mise à profit pour accélérer les négociations sur les **amendements à la convention de Budapest de 2001 du Conseil de l'Europe** sur la cybercriminalité et sur le **projet de règlement européen sur les preuves électroniques** (« *e-evidence* »), **et reprendre les négociations entre l'Union**

européenne et les États-Unis, afin de renforcer la coopération internationale contre la cybercriminalité **(proposition n°8)**.

Pour aider à la consolidation de l'écosystème français de la cyberprotection, **le droit de la commande publique doit évoluer :**

- en pérennisant les dispositions du décret du 24 décembre 2018 permettant aux collectivités locales de passer un marché sans mise en concurrence pour des « services innovants » ;
- en permettant l'accès à l'offre de cybersécurité en dehors des plateformes de grossistes ;
- et en étudiant la possibilité que les opérateurs de réseaux puissent privilégier un achat européen ou national de solutions de cybersécurité (**proposition n°4**).

Pour renforcer la cybersécurité des entreprises, le rôle des assurances est décisif.

Dans un premier temps, **l'assurabilité tant des rançongiciels que des sanctions administratives en cas de violation de la réglementation sur la protection des données à caractère personnel, doit être interdite,** à la fois au niveau européen et national (**proposition n°12**).

Dans un deuxième temps, **le marché de l'assurance doit être conforté :**

- par une **meilleure compréhension du risque,** en ayant la connaissance la plus exhaustive possible des sinistres ;
- par **l'utilisation de logiciels et d'experts en cybersécurité certifiés,** afin de promouvoir le **label *Expert Cyber*** ;
- par la **création d'une agence de cybernotation européenne, utilisant les référentiels** de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)**, ou française,** utilisant ceux de l'ANSSI **(proposition n°16)**

Dans un troisième temps, **l'éligibilité au remboursement d'un dommage lié à une cyberattaque par les assurances devra être subordonnée au recours à un prestataire labellisé *Expert Cyber* (proposition n°11).**

Des solutions simples et mutualisées à destination des PME et TPE

Pour **remédier** à la **pénurie** de ressources humaines en expertise, il faut **faciliter la mutualisation de responsables de sécurité des systèmes informatiques (RSSI) pour les PME,** par exemple par la constitution **de groupements d'employeurs** ayant un statut de tiers de confiance **(proposition n°17).**

Pour **simplifier** la vie des entreprises, il faut développer l'offre d'un **« *package* » de solutions de cybersécurité pour les TPE et PME (proposition n°18)** et notamment: étudier la faisabilité d'une **solution de démarrage rapide configurant l'usage du cloud aux prescriptions de cybersécurité définies par l'ANSSI. Par ailleurs, une approche commune franco-allemande pourrait plaider en faveur d'une meilleure prise en considération des PME** dans la stratégie commune européenne de cybersécurité dans le cloud, définie par l'ENISA **(proposition n°20).**

Pour **financer** cette mise à niveau en cyberprotection, il faut, comme le Sénat l'a préconisé à de multiples occasions, mettre en place **un crédit d'impôt à destination des TPE et PME. Celui-ci couvrirait une partie des dépenses d'équipement** (logiciels ou abonnement cloud) et de **formation des chefs d'entreprise et des salariés à la cybersécurité (proposition n°21).**

Pour **rétablir l'égalité** des relations contractuelles dans le cloud, il faut **accorder aux TPE et PME dont le champ de l'activité principale n'est pas le numérique, la protection de l'article L.212-1 du Code de la consommation sur les clauses abusives (proposition n°19).**

Proposition n°1 : Promouvoir davantage le dispositif *cybermalveillance.gouv.fr* auprès des entreprises et dédier un service d'urgence aux entreprises ; des étudiants disposant des compétences numériques adéquates pourraient y effectuer leur service civique.

Proposition n°2 : Ouvrir un guichet de recueil anonymisé des cyberattaques frappant les entreprises, afin de disposer de statistiques fiables.

Proposition n°3 : Décliner des équipes de réponse aux incidents informatiques (CSIRT, *Computer Security Incident Response Team*) dans les **Régions** et inclure la cybersécurité dans les schémas régionaux de développement économique, d'internationalisation et d'innovation (SRDEII) afin de sensibiliser les collectivités locales.

Proposition n°4 : Adapter le droit de la commande publique pour favoriser l'écosystème de la cybersécurité en :

- Pérennisant les dispositions du décret du 24 décembre 2018 au profit des collectivités locales permettant l'achat sans mise en concurrence de « services innovants » ;
- Permettant l'accès à l'offre de cybersécurité en dehors des plateformes de grossistes ;
- Étudiant la possibilité que les opérateurs de réseaux puissent privilégier un achat européen ou national de solutions de cybersécurité.

Proposition n°5 : Élaborer des plans nationaux de prévention des cyberrisques, afin de coordonner la réponse des pouvoirs publics et des acteurs privés en cas d'attaque numérique systémique affectant une part significative des entreprises quelle que soit leur taille. Des **exercices de simulation** devraient être régulièrement organisés.

Proposition n°6 : Renforcer la réponse pénale à la cybercriminalité :

- Développer la formation initiale et continue des magistrats en matière de cybercriminalité ;
- Augmenter les effectifs spécialisés en cybersécurité des forces de sécurité ;
- Doter les forces de cybersécurité de moyens financiers adéquats ;
- Étudier la faisabilité de la création d'un Parquet national de lutte contre le cybercrime ;
- Créer, à chaque degré de juridiction, une chambre spécialisée dans la lutte contre la cybercriminalité.

Proposition n°7 : Adapter les procédures pénales à la cybercriminalité et renforcer la coopération des institutions judiciaires avec l'ANSSI au-delà de la lutte contre le terrorisme.

Proposition n°8 : Accélérer les négociations européennes sur le projet de règlement sur la **preuve électronique** (« *e-evidence* ») **et reprendre les négociations entre l'Union européenne et les Etats-Unis,** afin d'approfondir la coopération internationale concernant la cybercriminalité.

Proposition n°9 : Prévoir que les salariés doivent se voir proposer une sensibilisation à la cybersécurité, dans le cadre de la formation professionnelle au numérique.

Proposition n°10 : Déployer une campagne massive de promotion des métiers de la cybersécurité, cofinancée par l'État et les acteurs privés du secteur.

Proposition n°11 : Réserver à terme l'éligibilité à un remboursement par les assurances aux entreprises ayant eu recours aux services des prestataires labellisés *Expert Cyber*.

Proposition n°12 : Interdire l'assurabilité tant des rançongiciels que des sanctions administratives en cas en cas de violation de la réglementation sur la protection des données à caractère personnel, par un amendement à la convention de Budapest du Conseil de l'Europe, par un règlement européen, et par une disposition législative expresse dans le code des assurances.

Proposition n°13 : Afin de renforcer la conception sécurisée (*security by design)* :

- étudier l'extension aux entreprises de la « garantie logicielle » concernant les mises à jour de sécurité ;
- organiser, avec le support de l'ANSSI, un « hackathon de la cybersécurité » des entreprises, lors de la Journée mondiale de la cybersécurité, le 30 novembre.

Proposition n°14 : Construire un référentiel accessible aux TPE et PME pour renforcer la **certification** en matière de cybersécurité.

Proposition n°15 : Sensibiliser les PME sur la responsabilité personnelle des dirigeants en cas de cyberattaque de la chaîne d'approvisionnement dont ils sont partie prenante.

Proposition n°16 : Affermir le marché de l'assurance en matière de cybersécurité par :

- Une meilleure compréhension du risque, en ayant la connaissance la plus exhaustive possible des sinistres ;
- L'utilisation de logiciels et d'experts en cybersécurité certifiés, afin de promouvoir le label ExpertCyber ;
- La création d'une agence de cybernotation européenne, utilisant les référentiels de l'Agence européenne chargée de la sécurité des réseaux et de l'information –ENISA-, ou française, utilisant ceux de l'ANSSI.

Proposition n°17 : Faciliter la mutualisation des responsables de la sécurité des services informatiques (RSSI) pour les PME, par exemple par la constitution de groupements d'employeurs, ayant un statut de tiers de confiance.

Proposition n°18 : Développer l'offre d'un « package » simplifié de solutions de cybersécurité aux TPE et PME.

Proposition n°19 : Accorder aux TPE et PME, dont le champ de l'activité principale n'est pas le numérique, la **protection** de l'article L.212-1 du Code de la consommation sur les **clauses abusives** pour les contrats conclus en matière de cybersécurité.

Proposition n°20 : Étudier la faisabilité d'une solution de démarrage rapide configurant l'usage du cloud aux prescriptions de cybersécurité définies par l'ANSSI et d'une approche commune franco-allemande en faveur d'une meilleure prise en considération des PME dans la stratégie commune européenne de cybersécurité dans le cloud, définie par l'ENISA.

Proposition n°21 : Mettre en place un crédit d'impôt à destination des chefs d'entreprise et des salariés des PME, prenant en charge une partie des dépenses d'équipement et de formation à la cybersécurité.

Proposition n°22 : Instaurer un cyberscore des plateformes numériques destinées au grand public, afin de sensibiliser les citoyens à la cybersécurité.

Serge Babary
Président
Sénateur (Les Républicains) de l'Indre-et-Loire

Rémy Cardon
Rapporteur
Sénateur (Socialiste, Écologiste et Républicain) de la Somme

Sébastien Meurant
Rapporteur
Sénateur (Les Républicains) du Val d'Oise

Délégation sénatoriale aux entreprises

Téléphone : 01.42.34.28.96 - delegation-entreprises@senat.fr

Consulter le rapport :

http://www.senat.fr/rapports-classes/crentr.html