Janvier 2019

Note de sensibilisation

CYBERSÉCURITÉ : UNE URGENCE À SE PROTÉGER

CESER Auvergne-Rhône-Alpes
Conseil Économique, Social & Environnemental Régional

Le Code Général des collectivités territoriales précise en son article L 4134-1 :

« Le conseil économique, social et environnemental régional est, auprès du conseil régional et du président du conseil régional, une assemblée consultative.

Il a pour mission d'informer le conseil régional sur les enjeux et conséquences économiques, sociaux et environnementaux des politiques régionales, de participer aux consultations organisées à l'échelle régionale, ainsi que de contribuer à des évaluations et à un suivi des politiques publiques régionales. »

Le CESER est l'assemblée consultative, représentative de la vie économique, sociale et environnementale de la région. Elle émet des avis (saisines) et contributions (autosaisines).

Expression de la société civile organisée dans toute sa diversité, les propositions du CESER éclairent les choix des décideurs régionaux.

Ainsi, le CESER concourt à l'administration de la région aux côtés du Conseil régional et de son Président.

Contribution n°2019-04

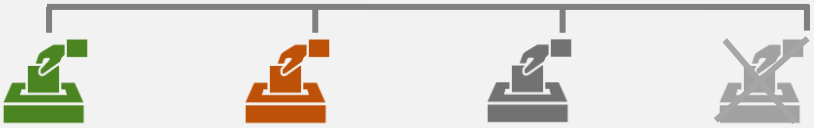
Président de commission

M. Éric LE JAOUEN

Commission n° 1
« Activités économiques, emploi et innovation »

RESULTATS DES VOTES

144 *votants*



143	1	0	0
ont voté **POUR**	ont voté **CONTRE**	s'est **ABSTENU.E**	n'ont pas pris part au vote

Cette contribution a été adoptée par le
Conseil, Economique, Social et Environnemental régional Auvergne-Rhône-Alpes
lors de son Assemblée Plénière du 23 janvier 2019.

Sommaire

Préambule

Forte de ses 190 conseillers issus de la Société civile, notre assemblée consultative a pour vocation première de permettre aux habitants de la Région de **vivre mieux**.

Internet est l'espace d'expression et d'échange qui regroupe aujourd'hui plus de la moitié de la population mondiale, avec une augmentation de 8 % par an.

Notre rôle est d'éclairer sur les évolutions annoncées et les défis majeurs de sécurité que posent les différents usages d'internet et qui nous concernent tous : institutions, entreprises, citoyens.

Comment assurer la sécurité des échanges et des transactions dans cet espace dématérialisé, sans frontières ni limites ? Comment se prémunir des préjudices liés à une professionnalisation des cyberattaquants et au développement des objets connectés ? Comment mieux protéger l'accès aux données personnelles et aux infrastructures stratégiques ?

Qui dit nouveaux risques, dit également nouvelles opportunités. En Auvergne-Rhône-Alpes, acteurs industriels, start-ups, centres de recherche et de formation peuvent se saisir de ce potentiel de développement économique et d'emploi.

La Commission 1 « Activités économiques, emploi et innovation » a fait le choix de présenter, pour la première fois, ses travaux sous la forme d'une note de sensibilisation. Ainsi, nous espérons vivement que le fruit des auditions et réflexions conduites au sein de notre assemblée, rassemblant ici alertes et propositions d'action, seront utiles à tous nos partenaires et acteurs du cyberespace..

Antoine QUADRINI,
Président du CESER Auvergne-Rhône-Alpes

Introduction

CONTEXTE

Captation d'informations sur la vie privée, surveillance des sites visités, intégrité des données stockées, prise de contrôle ou altération des systèmes d'information, détournement de flux financiers, piratage de messagerie, de comptes, usurpation d'identités, tels sont les grands enjeux de la sécurité du numérique.
Préoccupation relativement récente, la cybersécurité doit répondre à différents enjeux et prémunir de certains risques. La presse se fait l'écho d'un certain nombre de cyberattaques particulièrement marquantes. Par exemple en mai et en juin 2017, deux attaques massives ont marqué les esprits. Elles ont concerné notamment des constructeurs automobiles, opérateurs téléphoniques, hôpitaux, organismes financiers et infrastructures de transport. Demain, les véhicules autonomes et la généralisation des technologies numériques dans la santé seront des cibles particulièrement sensibles. D'autres menaces moins spectaculaires et médiatisées pèsent également sur l'ensemble des acteurs.

OBJECTIF

Cette note de sensibilisation sur la cybersécurité a pour objectif d'attirer l'attention des acteurs régionaux sur ce sujet. Il concerne l'ensemble des organisations : entreprises, associations collectivités et acteurs publics. Il concerne également les citoyens. Ils ne sont pas à l'abri de certaines attaques directement ou indirectement par les liens qu'ils entretiennent avec ces entités.

ENJEUX

Les menaces sont d'autant plus importantes que la surface d'exposition aux risques est croissante, compte tenu de l'augmentation, d'une part, des utilisateurs et des objets connectés, et de la diversité des cyberattaquants d'autre part, ce sera l'objet de la première partie.
Ce sont l'ensemble de ces risques et des enjeux qui en découlent que le CESER a souhaité identifier ici. Mais il ne s'agit pas sur ce thème d'apporter uniquement une vision anxiogène. Mais il convient d'insister sur le fait que la cybersécurité est la responsabilité de tous. Chaque objet connecté donc chaque utilisateur peut être le point d'entrée d'une cyberattaque. La sécurité est tout autant menacée par la professionnalisation des attaquants potentiels que par l'absence de protection élémentaire et de négligence qui peuvent être sources de difficultés majeures. Comme dans le domaine sanitaire, pour éviter la propagation de virus, des réflexes de base d'« hygiène numérique » doivent être acquis.
Au-delà des risques, la cybersécurité et son développement sont aussi sources d'opportunités pour le développement de solutions adaptées dont le potentiel économique est très important. Mieux identifier celles-ci à l'échelle européenne, nationale et régionale est un défi important. Les enjeux économiques s'entrecroisent ici avec des enjeux de nature politique, liés à la souveraineté nationale voir européenne, ce sera l'objet de la deuxième partie.

Il faut aussi porter à connaissance un certain nombre de réponses existantes au niveau national ou régional qui sont apportées aux acteurs pour faire face à ce risque, c'est ce qui sera développé dans la troisième partie.

DÉMARCHE

Enfin, cette note pointera quelques recommandations à destination des acteurs régionaux afin de mobiliser davantage et plus rapidement sur ce thème. Il s'agit aussi bien de se prémunir de cette nouvelle forme de délinquance que d'initier des solutions spécifiques en lien avec les particularités économiques du territoire régional. Il s'agit de proposer des pistes afin qu'une région comme Auvergne-Rhône-Alpes qui revendique une position et des atouts dans le secteur du numérique, puisse contribuer à cette problématique.

"Si vous pensez que la technologie peut résoudre vos problèmes de sécurité alors vous n'avez rien compris aux problèmes ni à la technologie".

Bruce SCHNEIER, Cryptologue, Spécialiste en sécurité informatique et écrivain américain

PARTIE 1 : Une surface d'exposition aux risques en croissance

DÉFINITION

La cybersécurité peut se définir comme tout ce qui touche aux usages défensifs et offensifs des systèmes d'information :

- tant pour ce qui est des contenants : les moyens techniques utilisés pour l'échange de données,
- que pour ce qui est de la protection et de l'attaque des équipements informatiques,
- que sur les contenus, c'est-à-dire les renseignements disponibles sur la toile : données personnelles…

Selon l'Institut eMarketer

En 2018, dans le monde, quelques **3,66 milliards** d'internautes.

En 2021, 4,13 milliards soit **53,6 %** de la population mondiale.

Le champ des menaces est aussi vaste que la présence et l'utilisation de ces technologies de l'information et de la communication dans toutes les structures de nos États, de nos entreprises, de nos collectivités, de nos associations, de nos maisons… Toutes sont des cibles potentielles, notre patrimoine informationnel est totalement exposé !

Jean-Claude JUNCKER, Président de la Commission Européenne, qui a fait de la cybersécurité une des cinq priorités de son mandat, avait alerté sur l'importance du sujet pour les sociétés démocratiques :

❝ Les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars. Elles ne connaissent pas de frontières, n'épargnent personne. ❞

Des attaquants aux motivations diverses

Les ingérences extérieures peuvent avoir plusieurs origines :

CYBER-ESPIONS	CYBER-ACTIVISTES	CYBER-DÉLINQUANTS
Au service de puissances étrangères	Avec des visées idéologiques	Avec des visées financières

L'espionnage et les interceptions

Le baromètre annuel[1] Euler-Hermes indique en mai 2018 que plus de sept entreprises sur dix en France ont fait l'objet d'une attaque de cyberfraude en 2017,-qu'une sur trois a subi au moins une fraude avérée et que 10 % des entreprises attaquées ont subi un préjudice moyen supérieur à 100 k€. Si entre 2016 et 2017 le nombre d'entreprises visées s'est légèrement réduit, le nombre de fraudes avérées a augmenté. **Cela traduit une professionnalisation des fraudeurs selon les spécialistes**.

Les informations ainsi recueillies peuvent servir à renseigner un concurrent ou se monnayer sur des places de marchés. On note aussi des attaques moins techniques, mais tout aussi lucratives, comme le phising ou hameçonnage. Une autre piste d'insécurité est la sous-traitance. En effet, l'entreprise ouvre ainsi des accès à son système d'information à des sociétés qui ne disposent pas forcément des mêmes pare-feux ; Par ailleurs, le recours à l'intérim et la généralisation du cloud-computing ou externalisation du traitement des données peuvent être des sources de danger.

Logiciels malveillants les plus couramment observés

Décompte	
87 329	Applications potentiellement indésirables et fichiers binaires suspects
50 081	Injecteurs de chevaux de Troie (VBS)
35 887	Liens Facebook frauduleux
27 627	Téléchargeurs de chevaux de Troie (Scripts)
24 737	Redirection du navigateur (JS)
18 505	Redirection du navigateur — Téléchargements
15 933	Phishing (Liens)
14 020	Chevaux de Troie Android (lop)
12 848	Redirection du navigateur
11 600	Piratages de profils Facebook
11 506	Blocages heuristiques (Scripts)
···7712	Binaires compressés
···5995	Téléchargeurs de chevaux de Troie (JS)
···5510	Chevaux de Troie, méthodes heuristiques (Win32)
···5467	Attaques iFrame du navigateur
···4970	Android (Axent)
···4584	Chevaux de Troie Android (Loki)
···4398	Malwares (FakeAvCn)
···3646	Chevaux de Troie (HideLink)
···3006	Malwares (HappJS)

Source : Rapport CISCO 2017

La déstabilisation et le sabotage informatique

La déstabilisation peut se traduire de plusieurs manières : propagande, fausses informations, atteinte à l'e-réputation, influence sur le net, maitrise de la mémoire collective. Les méthodes utilisées s'inspirent de méthodes ayant fait leur preuve avant l'ère numérique. Toutefois certaines méritent d'être développées.

Les attaques à la réputation sont des menaces de plus en plus fortes pour les entreprises.

L'estimation de la valeur des plus grandes marques ou noms (économiques ou autres) se chiffre en dizaine de millions de dollars : exemple Google, Coca-Cola … Dans ce contexte, les attaques à la réputation peuvent causer des dégâts financiers considérables. Internet démocratise la menace et expose les organisations et les personnes. Ces attaques informationnelles n'ont pas pour seule cible les grands groupes : des PME peuvent faire l'objet de campagnes de dénigrement. Certains secteurs sont plus exposés que d'autres.

[1] Leader européen de l'assurance fraude /DFCG (association nationale des directeurs financiers et de contrôle de gestion).

Les attaques visant une déstabilisation de la cible, peuvent aussi parfois se combiner avec de l'extorsion et du rançonnage : un pirate rançonne en menaçant de diffuser vos consultations sur internet …

Internet voit aussi se développer l'usurpation d'identité numérique qui est souvent un moyen de développer des attaques fortes. Dans son baromètre annuel [2], Euler Hermès souligne que si la fraude au faux président s'est ralentie, la fraude au faux fournisseur, aux faux banquiers, avocats ou commissaires aux comptes et au faux clients sont en augmentation forte.

Si la toile est une vitrine, **c'est aussi une caisse de résonnance fort utile pour les opérations d'influence.** Ainsi, en mai 2009, le tribunal de commerce de Paris a condamné Google à la demande de Direct Énergie : en raison de la fonction « suggest » qui propose à l'internaute des intitulés à partir des premières lettres d'un nom. De ce fait, dès que vous écriviez Direct Énergie apparaissait le mot « arnaque ».

Les « Fake news », informations délibérément fausses en sont aussi un exemple.

Le sabotage informatique est sans doute dans l'imaginaire commun, ce qui vient immédiatement à l'esprit lorsque l'on évoque le risque cyber : la capacité à prendre les commandes des systèmes d'information de sa cible, systèmes militaires, industriels ou urbains, dont les conséquences peuvent être très importantes.

La cybercriminalité : vol et extorsion d'argent notamment

En matière d'escroquerie, l'année 2017 a vu un net recul des Faux Ordres de Virement Internationaux (FOVI) et **la recrudescence d'autres types d'escroquerie** : sites frauduleux proposant des placements indexés sur le cours du diamant ou les escroqueries dites au faux support technique dont une nouvelle campagne a été détectée en novembre 2017.

Les fraudes à la carte bancaire poursuivent leur évolution. Les attaques de mai et juin 2017, Wannacry et NotPetya, ont eu un aspect inédit par leur dimension massive et internationale, la diversité des victimes touchées, l'ampleur de la propagation et les dommages causés de manière indiscriminée.

[2] En partenariat avec la DFCG (association nationale des directeurs financiers et de contrôle de gestion).

Comment se prépare l'ingérence ?

Ces ingérences s'appuient sur des méthodes bien structurées qui suivent toujours une trame commune :

1. **Leur action s'appuie d'abord sur l'identification de l'environnement** des personnes cibles à travers toutes les données disponibles sur le web et les réseaux sociaux sur la personnalité des personnes visées, leur centre d'intérêt. Ils cherchent à cibler les détenteurs des mots de passe : les administrateurs, les stagiaires et les rapports qui évoquent des points particuliers de l'entreprise.

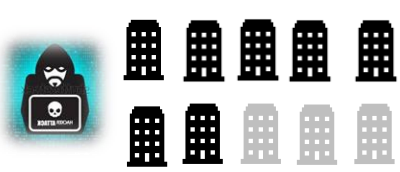
   Il faut, face à cela, développer une véritable culture d'hygiène informatique. Les mails, les clés USB notamment sont des moyens d'entrer dans les systèmes informatiques.

2. Le deuxième stade **visera à approcher les personnes en s'appuyant sur des pratiques d'élicitation**. L'*élicitation* désigne un ensemble de techniques qui permettent d'amener un interlocuteur à dévoiler des informations confidentielles. Les agresseurs identifient les leviers qu'ils peuvent actionner chez la personne : l'argent, l'idéologie, la compromission, le chantage, l'ego de la personne.

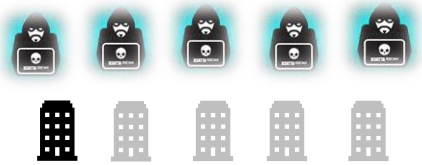
3. Enfin , il peut y avoir **un troisième stade qui vise à recruter la personne afin qu'elle participe de plein gré à l'ingérence.**

   Il faut noter que les prestataires informatiques sont des cibles privilégiées. L'ensemble des équipements informatiques connectés à internet (imprimantes, etc) sont des cibles et des points d'accès pour entrer dans le système. L'augmentation des objets connectés va intensifier les possibilités et donc les risques.

Des risques en croissance et une professionnalisation de la fraude



7 entreprises sur 10 ont été **victimes d'**(au moins) **1 tentative de fraude** sur l'année écoulée [1]



1 entreprise sur 5 a subi **plus de 5 tentatives de fraude** sur cette même période [1]

1 entreprise

sur 3

a subi au moins **1 fraude avérée** en 2017 [1]

30 % ont constaté une **recrudescence** particulière des attaques en **période de congés / week-end** [1]

TOP 3 DES TENTATIVES DE FRAUDES [1]

54%

Fraude au faux fournisseur

50%

(dont 20% d'attaques au ransomware)

Cyber-criminalité

43%

Autres usurpations d'identité (banques,avocats..)

QUELLES MENACES POUR LES ENTREPRISES ? [1]

85%

Risque financier

45%

Risque sur les données

30%

Risque d'interruption de l'activité/des opérations

29%

Risque de réputation pour l'entreprise

PRÉVISIONS

2015

70 % du trafic Internet mondial généré par la vidéo [2]

D'ici 2020

82 % du trafic Internet mondial généré par la vidéo [2]

2/3 des **mails** sont des **spams**

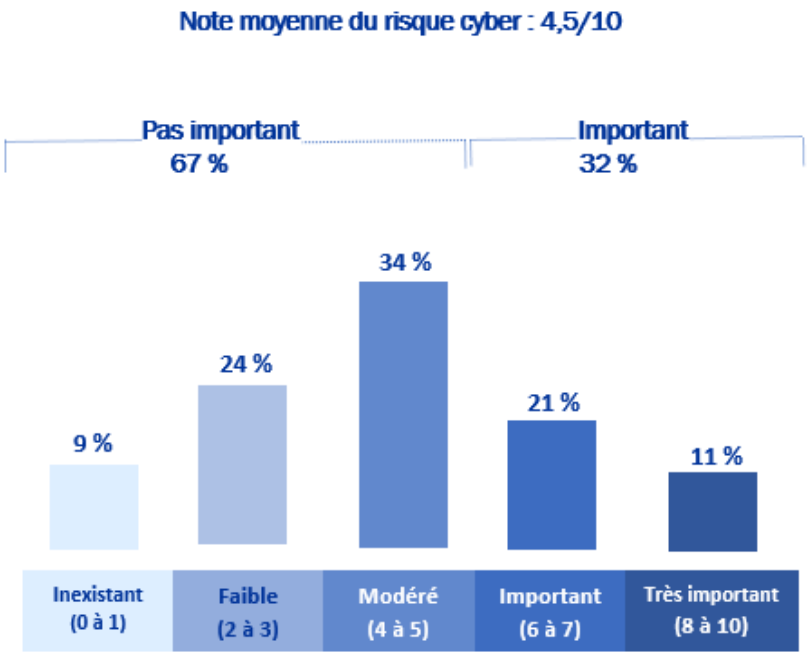
8 à 10 % des **spams** sont considérés comme des **produits malveillants** [2]

[1] Étude Euler Hermes – DFCG 2018

[2] Rapport annuel CISCO 2017 sur la cybersécurité

PARTIE 2 : Des enjeux politiques et économiques qui s'entremêlent

A l'échelle mondiale, l'Europe investit nettement moins que d'autres parties du monde : « L'Europe dépense actuellement six à sept fois moins que les États-Unis en matière de Cybersécurité », extrait du discours du Ministre de l'Intérieur, Gérard COLLOMB, lors du 10ème Forum International de la Cybersécurité, en janvier 2018, à Lille.



Source : Document PWC – Octobre 2018

Les entreprises françaises semblent, néanmoins, plus avancées. Seulement 9 % d'entre elles n'ont pas encore entrepris de changement dans leur processus. Toutefois, PWC indique[3] que seul un tiers des entreprises considère la cybersécurité comme un enjeu prioritaire sachant que les chiffres varient selon la taille de l'entreprise.et deux tiers des entreprises considèrent que ce risque n'est pas important.

La question pour une entreprise, n'est plus, aujourd'hui, de savoir si elle va être ou non confrontée au cyber-risque. Elle l'est d'ores et déjà.

Selon l'ANSSI, le coût des dommages directs se chiffre entre quelques millions et plusieurs dizaines de millions d'euros pour une seule cyber-attaque réussie.

Sans avoir un caractère exhaustif, l'étude menée sur l'ensemble des faits portés à la connaissance de la gendarmerie montre une tendance globale en hausse de 30 % par rapport à 2016 ; plus de 60 % du total de ces infractions sont des escroqueries liées à Internet.

L'évaluation du coût de la cybercriminalité reste encore un exercice complexe, bon nombre de victimes ne déposant pas plainte. Le coût estimé d'une violation de sécurité est en moyenne de plusieurs centaines de milliers euros pour une Entreprise de Taille Moyenne (ETI) et le préjudice moyen d'un détournement de données pour chaque entreprise victime porte sur plusieurs millions d'euros.

[3] Dans le baromètre d'octobre 2018 réalisé par IPSOS à sa demande concernant la cybersécurité.

Selon un sondage effectué auprès de 1 000 entreprises, le coût estimé d'une violation de sécurité serait en moyenne de 330 000 euros pour une entreprise de 1 000 salariés ou moins, et 1,3 million d'euros pour une entreprise de plus de 5 000 salariés.

Enfin, la Gendarmerie Nationale réalise depuis 2014 une étude des dossiers se rapportant à la cybercriminalité et qui font l'objet d'une remontée des « comptes rendus de police judiciaire ». Relevé dans ce contexte, le préjudice approximatif est estimé à 363 millions d'euros contre 286,6 millions pour l'année 2016 (+26 %).

Ces chiffres importants pèsent forcément sur la dynamique économique des entreprises mais au-delà de cela une attention particulière à la souveraineté numérique doit être portée, c'est un enjeu majeur pour l'indépendance de la France et de l'Europe.

L'Europe : une action limitée malgré des évolutions

L'Union européenne avait créé, dès 2004, une Agence chargée de la sécurité des réseaux et de l'information, l'ENISA : European Union Agency for Network and Information Security

Elle lui avait fixé **cinq missions** :

1. **Conseiller et assister la Commission et les États membres en matière de sécurité de l'information et les aider, en concertation avec le secteur, à faire face aux problèmes de sécurité matérielle et logicielle**
3. **Recueillir et analyser les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents**
3. **Promouvoir des méthodes d'évaluation et de gestion des risques afin d'améliorer notre capacité à faire face aux menaces pesant sur la sécurité de l'information**
4. **Favoriser l'échange de bonnes pratiques en matière de sensibilisation et de coopération avec les différents acteurs du domaine de la sécurité de l'information, notamment en créant des partenariats entre le secteur public et le secteur privé avec des entreprises spécialisées**
5. **Suivre l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information**

Or, l'ENISA n'a pas évolué depuis. Elle est restée une agence aux moyens réduits, dotée de seulement 80 salariés, et au mandat limité dans le temps, qui doit s'achever en juin 2020.

L'approche de la fin du mandat de l'ENISA a amené la Commission européenne à réfléchir au rôle futur qu'elle souhaitait lui donner. En 2016, l'Union Européenne avait pourtant fait évoluer son action en matière de cybersécurité et le rôle de l'ENISA avec l'adoption de la directive sur la sécurité des réseaux d'information. En effet, la directive NIS a été transposée en droit français au début de 2018 et a donné lieu à la mise en place du RGPD (Règlement Général pour la Protection des données).

Ainsi, l'ENISA prévoit que :

- Chaque État membre doit se doter d'une agence spécialisée dans la cybersécurité, à l'image de l'Agence Nationale pour la Sécurité des Systèmes d'Information en France, l'ANSSI.
- Le renforcement par chaque État de la cybersécurité d' « opérateurs de services essentiels » au fonctionnement de l'économie et de la société, les administrations, mais aussi les grandes entreprises et celles travaillant dans des secteurs sensibles. Et ces opérateurs auront l'obligation de signaler les attaques dont ils sont victimes.
- La participation volontaire à une coopération entre États membres.
- L'adoption de règles européennes communes en matière de cybersécurité pour certains prestataires de services numériques dans des domaines comme l'informatique en nuage pour le stockage des données, les moteurs de recherche et les places de marché en ligne.

Paquet cybersécurité

Signe de l'importance que la Commission Européenne accorde au sujet, la cybersécurité a été évoquée par Jean-Claude JUNCKER dans son discours sur l'état de l'Union le 13 septembre 2017. Dans la foulée, la Commission a annoncé une série de mesures surnommée « paquet cybersécurité » :

- Une communication chapeau intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide »,
- Une proposition de règlement sur l'ENISA, aussi appelé acte pour la cybersécurité,
- Une communication et une recommandation proposant un cadre européen de réponses aux crises cyber,
- Une communication précisant certaines modalités de mise en œuvre de la directive NIS sur la sécurité des réseaux et systèmes d'information.

La Commission Européenne rappelle que « la cybersécurité est essentielle tant pour notre prospérité que pour notre sécurité ». Cela concerne la cybercriminalité, dont l'incidence sur l'économie a quintuplé entre 2013 et 2017 et pourrait encore quadrupler d'ici à 2019.

Le CESE Européen s'est récemment prononcé sur ce sujet en proposant un certain nombre de mesures pratiques.

Parmi celles-ci, deux peuvent particulièrement retenir notre attention :

- ☑ L'importance du facteur humain sur ce thème tant en termes d'éducation et de protection,
- ☑ Créer un réseau européen de compétences en matière de cybersécurité.

La stratégie nationale pour la sécurité numérique

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

Créée en 2009, elle a une compétence nationale et transversale.

Elle met son expertise au service de l'administration et des opérateurs d'importance vitale.

Elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux, notamment par le pilotage du système français de certification de cybersécurité.

Le 21 juin dernier, l'ANSSI a d'ailleurs mis à l'honneur l'excellence française en matière d'évaluation de sécurité avec la première cérémonie de remise du Visa de sécurité.

En effet, face à la multiplicité des cyberattaques, d'un côté, et à la myriade de solutions de cybersécurité, de l'autre, les acteurs sont perdus. L'objectif est « de rendre plus accessible à tous - et en particulier aux petites structures comme les TPE/PME et même les collectivités locales - les solutions de cybersécurité les plus sécurisées », a précisé le secrétaire d'Etat chargé du numérique.

Et comme l'enjeu est européen, un visa européen va voir le jour suite à la décision du Conseil de l'Europe du 8 juin dernier. Le visa européen devrait voir le jour d'ici trois ans.

Le Ministère des Armées

Au Ministère des Armées, un commandement de cyberdéfense (ComCyber) a été créé en janvier 2017 :

Il rassemble l'ensemble des forces de cyberdéfense des armées françaises sous une même autorité opérationnelle, permanente et interarmées,

Ses trois missions principales sont le cyber-renseignement, la cyber-protection et les opérations cyber-offensives.

Le Ministère de l'Intérieur

Le Ministère de l'Intérieur a institué en 2017, un Délégué Ministériel aux Industries de Sécurité et à la Lutte contre les Cybermenaces. Il a pour mission d'élaborer une stratégie ministérielle de lutte contre les cybermenaces et de coordonner sa mise en œuvre. Il pilote son évaluation et son actualisation. Il est à noter que dès décembre 2013, l'Article 22 de la loi de programmation militaire impose aux OIV (Opérateurs d'Importance Vitale) le renforcement des systèmes d'informations critiques qu'ils exploitent.

La France a été le premier pays européen à s'appuyer sur les réglementations pour mettre en place un dispositif obligatoire de protection de ces infrastructures critiques. Plus de 200 opérateurs publics ou privés dont les activités sont indispensables au bon fonctionnement et à la survie de la Nation sont concernés.

Il complète l'action de la sous-direction de la lutte contre la cybercriminalité, créée le 29 avril 2014.

Le Ministère de l'Intérieur, par sa présence dans les territoires, est un acteur majeur de la sensibilisation des particuliers, des acteurs économiques et des collectivités territoriales.

Les services du Ministère de l'Intérieur ont participé tout au long de l'année 2017, à de nombreux salons, rencontres et conférences, ouverts au public, au cours desquels les problématiques liées aux cybermenaces sont abordées.

Les mesures préventives ont pour objectif d'anticiper les menaces et de protéger les acteurs économiques a priori contre les risques et dangers numériques auxquels ils sont exposés.

Le ministère de l'Intérieur a renforcé les compétences des référents sûreté de la préfecture de police, de la gendarmerie et de la police nationales, présents au niveau territorial, afin qu'ils permettent aux entreprises qu'ils conseillent, de mieux se prémunir également contre la cybercriminalité.

En 2017, la Direction Générale de la Sécurité Intérieure (DGSI) a organisé près de 1 550 conférences sur la protection de l'information et la sécurité numérique, notamment à l'endroit des entreprises et institutionnels.

La Sous-Direction de Lutte contre la Cybercriminalité (SDLC) de la Direction Centrale de la Police Judiciaire (DCPJ) participe aussi activement à cet effort de sensibilisation.

Grâce à son maillage territorial, le Service Central de Renseignement Territorial (SCRT) joue un rôle de soutien et de capteur au profit des services spécialisés en charge de l'intelligence économique, dans le respect des attributions des services de l'État, de celles des ministères compétents et en lien avec les préfets de région, au coeur du dispositif.

La police et la gendarmerie disposent également d'unités dédiées.

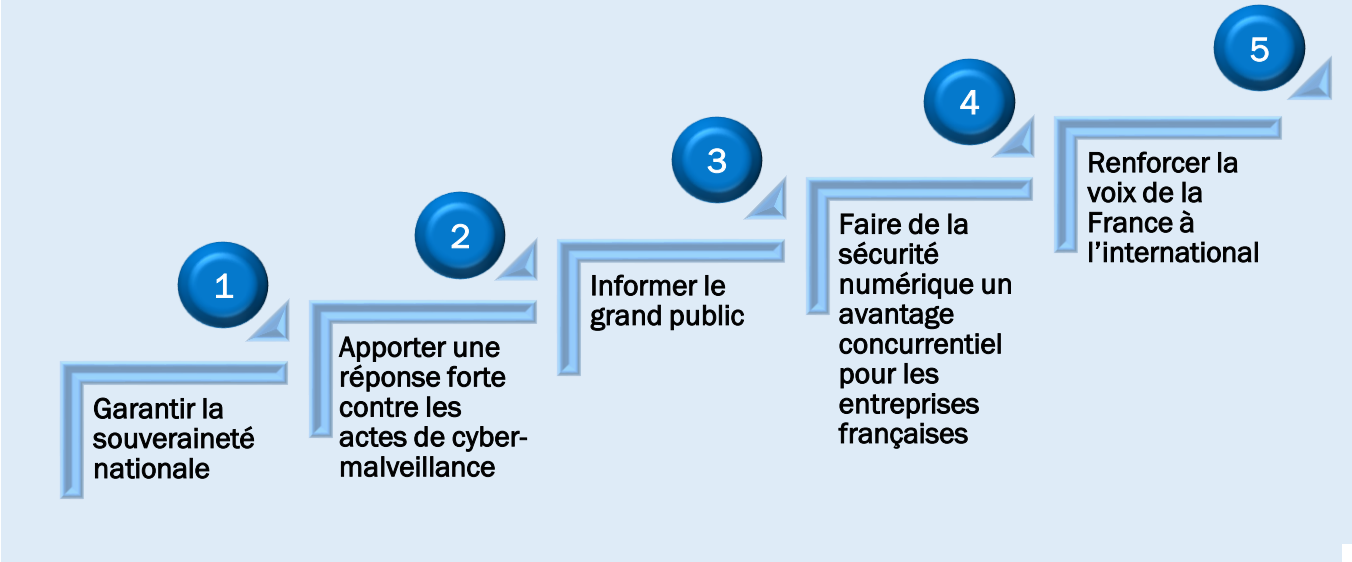
À titre d'exemple, le réseau Cybergend de la Gendarmerie Nationale dispose ainsi d'effectifs aux niveaux national, régional et local qu'elle prévoit de doubler d'ici à 2022.

Enfin, il convient de mentionner la création d'un poste d'ambassadeur pour le numérique occupé depuis le 22 novembre 2017 par David MARTINON auquel a succédé le 15 novembre 2018 Henri VERDIER.

Au cours des dernières années, la France a également fait évoluer sa stratégie en matière de cybersécurité.

À la Stratégie nationale pour la sécurité du numérique du 16 octobre 2015, s'est ajoutée la stratégie internationale de la France pour le numérique et la revue stratégique de cyberdéfense.

La Stratégie nationale pour la sécurité du numérique fixait cinq objectifs :



La Stratégie internationale de la France pour le numérique fixe notamment des objectifs en matière de cybersécurité pour garantir la sécurité et l'autonomie de la France dans le monde numérique. Elle prévoit aussi deux objectifs de portée européenne : renforcer les capacités des Européens en matière de cybersécurité et renforcer l'industrie et les services européens dans le secteur de la cybersécurité.

Lors de la rencontre de l'IGF[4] qui s'est tenue à Paris du 12 au 14 novembre et placée sous le signe de l'Internet of trust (Internet de confiance), le gouvernement français a lancé un appel pour inciter les entrprises et les Etats à collaborer pour instaurer un climat de confiance et de sécurité dans tout ce qui touche au numérique. L'objectif est de lutter contre la cybercriminalité sous toutes ces formes. Cet appel a été signé par plus de quarante pays.

[4] L'Internet Global Forum.

Le RGPD, un accélérateur dans la prise de conscience

Qu'est ce que le RGPD ?

L'acronyme RGPD signifie « Règlement Général sur la Protection des Données », il s'agit de la transposition en droit français de la directive européenne NIS (Network and Information Security) sur la sécurité des réseaux et des systèmes d'information. Cette transposition est effective depuis février. Il ya donc une obligation de mise en conformité avec le RGPD.

Qui est concerné par le RGPD ?

Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.
En effet, le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :
Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes.
Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.

D'après le Ministère de l'Intérieur, l'arrivée du RGPD a eu tendance à faire prendre conscience des enjeux de la cybersécurité. Avec la perspective d'amendes « pouvant aller jusqu'à 4 % du chiffre d'affaires mondial consolidé, une incitation forte repose maintenant sur l'écosystème des services et produits de cybersécurité », souligne le rapport. Car jusqu'à maintenant, cet enjeu représentait moins de 5 % du budget des technologies de l'information dans deux tiers des entreprises. Le RGPD oblige notamment faire la publicité des attaques en ligne subies, pour l'instant cela était plutôt caché auprès des fournisseurs et des clients.

Il a permis de refonder la gouvernance de la cybersécurité dans une entreprise sur deux.

Bilan du RGPD

Du côté des **professionnels** : une appropriation progressive

24 500 organismes ont désigné un délégué à la protection des données (personnes physiques ou morales) ; ce qui représente 13 000 DPO contre 5 000 CIL (correspondants informatique et libertés) avant le RGPD

Plus de **600 notifications de violations** de données ont été reçues, concernant environ 15 millions de personnes – soit environ 7 par jour depuis le 25 mai

Un volume toujours important de **demandes d'autorisation « santé »** : plus d'une centaine de demandes reçues, notamment en matière de recherche

Une hausse significative des contacts avec les publics, notamment les professionnels : **+ 45% d'appels sur les 7 premiers mois de 2018** ; + 83% de consultations des FAQ en ligne

3 millions de visites sur le site de la CNIL depuis mai 2018

150 000 téléchargements du modèle de registre simplifié proposé par la CNIL

Du côté des **particuliers** : une prise de conscience inédite

Depuis le 25 mai dernier, la CNIL a reçu 3767 plaintes contre 2294 plaintes sur la même période en 2017, qui constituait déjà une année record. Cela représente **une augmentation de 64%** et témoigne du fait que les citoyens se sont fortement saisis du RGPD. Ceci est sans doute consécutif à un coup de projecteur médiatique important récemment sur la protection des données : RGPD, Cambridge Analytica, etc

Deux organismes ont saisi la CNIL de **plaintes collectives**: la Quadrature du Net (Google, Amazon, Facebook, LinkedIn et Apple) et l'association NOYB (Google).

Les autorités de protection européennes traitent actuellement en coopération plus de **200 plaintes transfrontalières** et la France est autorité concernée pour une majorité d'entre elles. Ces plaintes soulèvent notamment des questions sur le consentement en général et notamment celui des mineurs

Source : Bilan de la CNIL après 4 mois de RGPD, https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application

La cybersécurité : une filière à fort potentiel

Dans ce contexte, le marché de la cybersécurité est en croissance continue.

Le rapport 2017 de l'observatoire de la filière de la confiance numérique, étude commanditée par l'Alliance pour la Confiance Numérique (ACN) dans le cadre de son observatoire 2017 – 82 entreprises y ont contribués. Cela couvre le marché de la cybersécurité proprement dite et des produits et solutions de sécurité numérique. On estime que ce secteur représente plus de 850 entreprises. 80 % de ces sociétés réalisent moins d'un million d'euros de chiffre d'affaires. Au total, la cybersécurité représente un chiffre d'affaires de 4,3 M€ et la sécurité numérique (16) 4,5 M€. La croissance annuelle moyenne du secteur est forte (12,4 %). Le nombre de personnes employées dans le secteur est estimé à 60 000.

Il s'agit donc d'une filière d'avenir que les Régions doivent accompagner économiquement mais aussi en termes de formation et de sensibilisation aux enjeux.

Une question de souveraineté et de confiance numérique

Pour asseoir sa souveraineté numérique, la France doit se doter d'une véritable stratégie industrielle.

Une telle démarche passe par l'identification des objectifs à atteindre en matière d'offre industrielle nationale ou de la confiance pour répondre aux besoins de la nation.

Il faut donc créer une base industrielle nationale ambitieuse en s'appuyant sur les poids lourds français déjà en place. La question du stockage des données sur des serveurs localisés en France ou en Europe est également une question stratégique fondamentale.

Aujourd'hui, il faudrait :

- favoriser l'émergence d'entreprises de taille intermédiaire dans ce secteur,
- soutenir les entreprises innovantes dans ce secteur,
- renforcer la coopération européenne pour construire une base industrielle de cybersécurité européenne, mais aussi
- œuvrer à la certification et à la qualification des produits performants

Trois grandes entreprises françaises font partie des leaders européens, voire mondiaux :

- **Thalès** : le spécialiste de la protection des données et du chiffrement, qui investit plus de 20 % de son chiffre d'affaire dans la recherche et le développement ;
- **Orange**: l'opérateur des télécommunications a développé depuis 2016, une branche consacrée à des activités de cybersécurité dédiées aux entreprises ;
- **Atos** : une des dix plus grandes entreprises du numérique à l'échelle mondiale, le groupe, figure parmi les leaders européens de l'informatique en nuage[5], de la cybersécurité et du supercalcul, ainsi que du paiement sécurisé en ligne pour les entreprises.

[5] Expression française pour cloud computing.

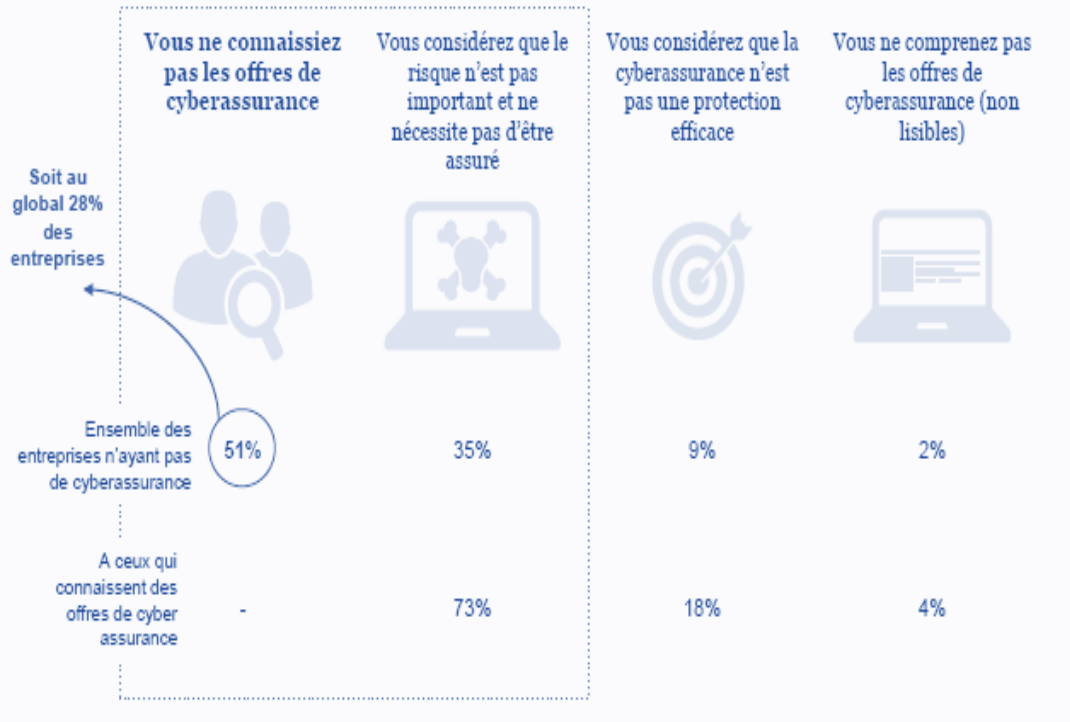
Parallèlement, des acteurs français spécialisés dans le numérique se sont réunis au sein d'associations, parmi lesquelles :

- **L'Alliance pour la confiance numérique**, qui a pour vocation de fédérer les principaux acteurs français et européens de la confiance numérique et de contribuer à la consolidation de la filière sécurité, que ce soit des entreprises de toute taille ou des centres de recherche ;
- **Hexatrust** qui rassemble des PME, des Entreprises de Taille Intermédiaire et des Start-Ups travaillant dans la cybersécurité et l'informatique en nuage et très implantées en Europe.

Autres axes de développement économique : créer un mécanisme assurantiel pertinent

L'assurance cyber peine aujourd'hui à s'imposer. Dans une entreprise le risque cyber doit être vu comme un risque parmi tant d'autres, considéré sous un angle économique, propice à son assurabilité.

Pour les assureurs, l'absence de données de référence sur le risque cyber, ainsi que son caractère potentiellement systémique constituent des difficultés aujourd'hui non surmontées.



Par ailleurs, la « non action » des opérateurs devient désormais une faute de gestion. Elle peut entraîner la responsabilité d'un dirigeant en cas d'incident cyber impactant significativement les résultats de son entreprise.

Or, en France, et plus généralement en Europe, le marché de l'assurance cyber demeure embryonnaire et représente moins de 10 % du marché mondial.

Il faut aussi développer les capacités des forces de sécurité du système judiciaire pour répondre à l'explosion du nombre de délits.

PARTIE 3 : Des réponses opérationnelles à disposition des acteurs

Pour faire face aux interrogations des différents acteurs, des réponses ont été mises en place.

Si la cybersécurité est un facteur de productivité, de compétitivité et donc de croissance pour les entreprises, pour les acteurs publics, c'est une condition pour l'exercice de missions de service public sécurisées. Pour les associations, c'est une condition pour l'exercice de leurs activités de manière sereine.

Les contraintes financières des petites structures restent un frein à la construction d'une cybersécurité optimale. Toutefois, il existe des bonnes pratiques peu coûteuses et faciles à mettre en œuvre. Il convient donc de diffuser une véritable culture de la sécurité auprès de tous les échelons. Des initiatives en ce sens ont déjà été prises tant au plan national que régional. Il convient de les souligner ici.

Au plan national

Ainsi, l'ANSSI publie des guides comme le « Guide des bonnes pratiques de l'informatique », réalisé avec la CPME qui présente des recommandations. Elle publie aussi des référentiels d'exigence. De manière générale, les organisations professionnelles mettent en place des démarches de sensibilisation des entreprises, on peut citer le MEDEF avec un test en ligne relatif à la mise en œuvre du RGPD, l'UNAPL avec l'édition d'un guide et l'organisation de formations sur la cybersécurité. CCI France soutient la démarche « Tour de France de la Cybersécurité » lancé en 2018 par le Cybercercle. En 2019, 7 villes seront concernées, Lyon en octobre, pour une journée organisée autour de tables rondes, de Master Class, d'ateliers et aussi d'un espace de rencontres-démonstrations, de rendez-vous individualisés au service de la filière cybersécurité locale, et d'un espace dédié aux formations et recrutement.

Toutefois pour de nombreuses TPE-PME et particuliers, la réponse n'est pas évidente. C'est pour répondre à cette problématique que l'Etat a lancé également, il y a un an, la plateforme ***Cybermalveillance.gouv.fr.***

Outre une fonction pédagogique (avec un kit de sensibilisation), la mission originelle de celle-ci est de mettre en relation les entreprises et particuliers victimes d'un acte de malveillance numérique avec des prestataires spécialisés dans ce domaine.

Par ailleurs, concernant **les fake news,** une loi en préparation dite loi contre la manipulation de l'information a été adoptée en première lecture à l'Assemblée Nationale. Il faut rappeler que les fake news ciblent autant les entreprises, les associations que les individus.

Sur le champ de la formation et des compétences, il faut citer la démarche initiée par l'OPIIEC (Observatoire Paritaire du Numérqiue, de l'Ingénierie, des Études et Conseil, et des Métiers de l'Évènement), qui dresse un état des lieux de l'offre de formation au plan national et propose un plan d'actions sur le sujet.

Un plan d'accompagnement des PME/TPE vers la numérisation, mis en place par l'Etat en partenariat avec Régions de France, dans lequel figure la question de la cyber-sécurité

Conscient du retard numérique des TPE-PME françaises, la France est au 16ème rang européen pour l'utilisation du numérique pour le commerce, l'industrie, Mounir MAHJOUBI, secrétaire d'Etat en charge du numérique a lancé le 15 octobre 2018 France Num un dispositif d'appui ciblé sur les entreprises de moins de 50 salariés, afin de leur permettre de faire « les premiers pas » décisifs en matière de numérisation de leur activité. Ce dispositif lancé en partenariat avec Régions de France vise à accélérer la transformation numérique des TPE et PME.

Au-delà d'une marque qui se veut fédératrice, France Num s'appuie notamment sur **un réseau de conseillers au niveau national**. Plus de 900 "Activateurs" répartis sur l'ensemble du territoire ont ainsi déjà été identifiés pour accompagner les entreprises qui souhaitent réaliser leur transformation numérique. Pour repérer ces activateurs, les TPE/PME pourront s'appuyer sur une plateforme de ressources personnalisées. Les entreprises pourront également y trouver les événements et les rencontres organisés localement, les offres de financement, ainsi que de recommandations. Autre axe majeur de France Num : la **nouvelle offre de prêts**. La BPIfrance et la BEI apporte leur garantie aux banques commerciales pour proposer des prêts très avantageux dédiés au développement numérique des entreprises. Conçue conjointement par les Régions de France et l'État qui en assureront le pilotage, France Num regroupe **plus de 25 partenaires**, parmi lesquels l'Arcep, Business France, Bpifrance, Syntec Nymérique, le Medef, la Banque de France…

La Commission Nationale Informatique et Libertés (CNIL)

La Commission Nationale de l'Informatique et des Libertés, met à disposition un logiciel libre PIA[6] afin d'accompagner les entreprises dans leurs analyses d'impact sur la protection des données dans le cadre de la mise en œuvre du règlement européen sur la protection des données.

Par ailleurs **plusieurs sites** ont été conçus au service des acteurs. Ils déploient des réponses.

www.ssi.gouv.fr

Site de **l'Agence Nationale de la Sécurité des Systèmes d'Information**

Vous retrouverez l'ensemble des **guides et référentiels de bonne pratique** en matière informatique, sous format pdf et de **MOOC (formation en ligne).** Guide d'Hygiène Informatique, Maîtriser les risques liés à l'infogérance (et donc cloud computing), la Cybersécurité des Systèmes Industriels, Voyager à l'étranger avec ses données professionnelles, **Guide d'élaboration d'une Charte Informatique**, etc. Ainsi que des notices pratiques (sécuriser son navigateur internet Firefox, anticiper les attaques en déni de service…) et la liste des **outils et prestataires qualifiés/certifiés par l'Etat.**

www.cert.ssi.gouv.fr

Site **secondaire de l'ANSSI**

Il émet des bulletins d'alerte quotidiens sur les **failles** et les **vulnérabilités** découvertes dans le numériques. Ces avis renvoient vers les **correctifs** associés et permettent de recouper les invitations de mise à jour de vos logiciels et de vos systèmes. A conseiller également : les **bulletins d'actualité** sur l'évolution des menaces, les **notices de recommandations** (la politique de mots de passe, l'administration de la messagerie, etc) ainsi que la rubrique « Que faire en cas d'intrusion ? ».

www.internet-signalement.gouv.fr

Portail gouvernemental permettant de **signaler les tentatives d'escroqueries en ligne ou tout type de contenu numérique illicite**, pour aider les enquêteurs spécialisés. Attention, il ne s'agit en aucun cas d'un site de dépôt de plainte en ligne. Par ailleurs, des rubriques de conseils et prévention sont également disponibles.

[6] Privacy Impact Assessment

www.cnil.fr

Site officiel de la **l'Agence Nationale de la Sécurité des Systèmes d'Information**

La Commission Nationale Informatique et Libertés est chargée de veiller à la loi du 6 janvier 1978 sur la protection des données à caractère personnel. A la fois **portail de déclaration** – obligation pour certaines !- et centre de ressources documentaires, on y trouve notamment de très bons **guides synthétiques et des voies de recours en cas d'atteinte à caractère individuel** (droit à l'oubli, suppression de contenus sur le web). A conseiller : le générateur de modèles de courrier, ainsi que les référentiels « pour les employeurs et les salariés » / « sécurité des données personnelles » / « mesures pour traiter les risques… » RAPPEL : **la démarche de droit à l'oubli sur l'internet** peut être complétée par une action via le site gratuit (pour l'instant) : www.forget.me

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

www.entreprises.gouv.fr/information-strategique-sisse

Site officiel de **Délégation Interministérielle à l'Intelligence Economique (D2IE)**

C'est surtout un portail de ressources documentaires où l'on trouve notamment un guide de **22 fiches thématiques consacrées à la sécurité économique**, le Guide du Routard de l'IE, **les flashs d'information de notre direction** et surtout les **outils d'auto-diagnostic** sur les principaux risques encourus (kits DIESE). Il convient de noter que ces ressources se déclinent spécifiquement au domaine de la **recherche scientifique**.

Information stratégique SISSE

www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs

Portail gouvernemental du **Ministère des Affaires Étrangères**

Il vise à faciliter la préparation et le bon déroulement de votre séjour à l'étranger. Il offre une **consultation par pays**, exposant les actualités de dernière minute, les contextes sécuritaire et sanitaire, les conditions d'entrée et de séjour, et toutes informations utiles (état des infrastructures, us et coutumes…) afin de limiter l'exposition aux risques. A noter la rubrique « Voyages d'affaires » et la **possibilité de signaler gratuitement son déplacement au M.A.E par le biais du service ARIANE.**

www.stopransomware.fr

Site associatif

Il vulgarise les problématiques liées aux « ransomwares » ou **rançongiciels**, typologie d'attaques qui prend en otage votre machine ou vos données, sous couvert d'un chantage à la clé de chiffrement.

www.nomoreransom.org

Site de la **Police Européenne**

www.sgdsn.gouv.fr

Site gouvernemental du **Secrétariat Général de la Défense** et de la **Sécurité Nationale**

Il a en charge de la coordination des actions de défense et de cyberdéfense (ressources sur le **plan Vigipirate, les Seteurs et Opérateurs d'Importance**

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

www.legalis.net

Site recensant les **actualités et jurisprudences liées au droit des nouvelles technologies**

Il est très intéressant pour ce qui relève des droits et obligations de l'employeurs et des employés, et du règlement judiciaire de litiges technologiques.

LEGALIS

www.hexatrust.com et www.francecybersecurity.fr

Portails respectifs de **deux initiatives privées (ETI – Entreprises – Consultants) ayant pour objectif commun de promouvoir les solutions françaises de cybersécurité**, et d'accroître la visibilité de ces offres à l'international. Concernant la deuxième association, une commission d'experts délivre un **label sur les produits SSI** qui lui sont soumis, ce label venant apprécier le respect de critères favorables aux intérêts hexagonaux. Un catalogue réactualisé chaque année est disponible en libre téléchargement.

CYBERSECURITY & DIGITAL TRUST ALLIANCE
HEXATRUST

Au plan régional

Une collectivité régionale qui se préoccupe fortement du sujet tant du point de vue de ses propres risques que de l'impulsion de solutions pour les acteurs régionaux

La Région Auvergne-Rhône-Alpes a fixé la sécurité comme un axe majeur de sa politique. Elle intervient en ce sens dans le cadre de ses compétences en matière de transport (TER), de politique en faveur des lycées et en direction des collectivités. Plusieurs actions visent notamment à développer la vidéo-surveillance. Or ces services nécessitent des moyens et supports « cyber ». Des infrastructures sont à mettre en place dans ce domaine avec l'objectif de développer les compétences et la culture des systèmes de sécurité informatique en Auvergne-Rhône-Alpes.

La Région s'engage aussi dans le soutien aux opportunités de développement que procure la cybersécurité. La Région a initié le campus numérique : pôle de formation et d'excellence numérique qui intègre cette dimension relative à la cybersécurité notamment à travers une collaboration avec le CNAM. Par ailleurs la Région participe à la création du Pôle Européen pour la sécurité Globale et le pôle de compétitivité SAFE d'Aix en Provence qui s'implique sur 4 enjeux : la formation, le développement industriel, la recherche et l'animation de l'écosystème de la sécurité. Il s'agit de favoriser l'implication des acteurs locaux dans cette dynamique.

Par ailleurs, la collectivité régionale qui développe la numérisation et la dématérialisation a entamé une démarche interne de sécurisation des données sensibles tant pour les données relatives aux exigences de gestion interne que de celles liées aux compétences de la collectivité qui relèvent de missions de services publics et des modes de gestion afférents comme les marchés publics. Malgré une connaissance des enjeux, elle pointe une compréhension et une acceptation des risques limités à l'intérieur de son organisation. Elle identifie des enjeux sociétaux pour l'ensemble des acteurs. En effet, l'accompagnement de la transformation numérique doit intégrer les nouveaux enjeux : travail à distance, protection des données personnelles et développement de l'accès numérique à l'administration et aux services. Autant de défis en matière de cybersécurité pour une région qui possède une surface large avec plus de 10 000 agents et plus de deux millions d'utilisateurs des services numériques régionaux. La Région a engagé un plan d'action et un schéma directeur de la sécurité

informatique. Elle a nommé un délégué à la protection des données et un responsable de la sécurité informatique.

Dans le cadre de son action en matière de numérique éducatif qui passe aussi bien par le financement d'infrastructures de communication, d'équipements informatiques, de l'accès à internet, de l'assistance déployée, de la mise en œuvre des Espaces numériques de travail (ENT), elle a engagé un processus de remplacement des passerelles de sécurité (320 au total). Il s'agit de protéger les accès aux ressources informatiques des lycées, à une meilleure détection des incidents de sécurité, de la rationalisation de l'usage de la bande passante et d'une détection facilitée des usages illicites.

Concernant ses compétences en matière de développement économique, la région Auvergne-Rhône-Alpes accompagne la numérisation des entreprises à travers le dispositif ambition PME et son volet numérique.

Le regroupement, à l'initiative de la Région, de l'ensemble des acteurs (Entreprises et Numérique ENE, Chambres consulaires, MEDEF, CPME, Imaginove, Minalogic, Digital League.) accompagnant les entreprises sur le champ numérique à travers le portail ma solution numérique : https://ma-solution-numerique.fr/ qui permet aux entreprises de trouver des solutions pour le développement de la numérisation et notamment sur la cybersécurité.

ECC4IU (EUROPEAN CYBERSECURITY CLUSTER FOR INDUSTRIALS AND URBANS SYSTEMS) : Un cluster spécialisé sur la cybersécurité des systèmes industriels et urbains

Il s'agit d'un cluster sur la sécurité des systèmes industriels et urbains : un levier pour regrouper les acteurs de la filière et innover en région. Initier par les industriels du secteur et la Métropole, le cluster a cinq objectifs opérationnels :

- Rédaction de guides opérationnels, cas d'usages métiers, livres blancs,
- Organisation d'événements de sensibilisation, d'animation et de promotion,
- Animation d'ateliers thématiques (détection d'intrusion, rédaction de cahiers des charges…),
- Organisation d'ateliers interdisciplinaires (assureurs, juristes…),
- Participation à des projets collaboratifs.

Cybersécuriser des systèmes industriels et urbains, c'est veiller à la sécurité du quotidien, l'eau, l'électricité, etc.

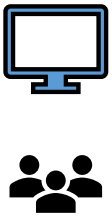
Des publications montrent que si en deçà de 5 jours, en cas d'incidents majeurs à l'échelle d'une ville(eau, électricité..) les hommes arrivent à s'entendre, au-delà les risques d'affrontement sont majeurs.

En 2014, l'État français a légiféré à travers la loi de programmation militaire pour les secteurs sensibles. Les grandes entreprises s'organisent mais pour les ETI, PME c'est plus difficile, aujourd'hui les équipements sont connectés à travers le tout numérique, l'industrie, la smart-city et l'hôpital.

Les cyberattaques ont des répercussions réelles : des usines qui s'arrêtent, des hôpitaux qui doivent fermer le bloc opératoire. Il faut mettre en œuvre des solutions qui ne sont pas uniquement technologiques.

TOP DES 3 DES SOLUTIONS MISES EN PLACE PAR LES ENTREPRISES AYANT ENGAGÉES UNE ACTION

87%



Sensibilisation des équipes, formations internes

80%

Renforcement des procédures de contrôle interne

44%

Risque de réputation pour l'entreprise

Le cluster est spécialisé dans les systèmes urbains et industriels et regroupent les opérateurs de systèmes industriels et urbains, des sociétés spécialisés dans l'assistance à maîtrise d'ouvrage et d'œuvre, des intégrateurs de solutions, des fournisseurs de solutions, des organismes de de formation et des sociétés de services d'assurances ou juridiques. Sur le champ de la sécurité des réseaux informatiques la région Bretagne a développé une filière reconnue. Sur le champ de la sécurité des systèmes industriels et urbains, compte tenu de la structure économique d'Auvergne-Rhône-Alpes, de la présence de nombreuses industries (chimie, nucléaire…) sensibles et de nombreux acteurs de la cybersécurité, des pistes méritent d'être explorés.

Le Grenoble Alpes Cybersecurity Institute

Le Grenoble Alpes cybersecurity Insititute est un projet issu de l'initiative Cross-Disciplinary Program de l'IDEX de l'université. Grenoble Alpes. Inauguré le 27 novembre, il vise à entreprendre des recherches interdisciplinaires novatrice afin de relever les défis de cybersécurité et de le protection de la vie privée. Les principaux axes de recherche sont :

- Les éléments sécurisés à bas coût,

- Les infrastructures critiques sécurisées et leur gestion en termes de cycle de vie,
- L'analyse de vulnérabilité et les défis globaux en termes d'analyse des risques et de validation des grands systèmes, incluant la capacité à faire face à certains dommages, soit la résilience pratique dans l'industrie et la société.

L'approche proposée englobe des aspects techniques, juridiques, économiques, sociaux, diplomatiques, militaires et de renseignements en partenariat avec le secteur privé et avec des coopérations nationales et internationales Il réunit plus d'une centaine de chercheurs de la région Rhône-Alpes. L'institut est le prolongement de réseaux existants comme AMNECYS (Alpine Multidisciplinary NEtwork on CYbersecurity) désigné comme l' un des principaux groupe de recherche français sur les enjeux du numérique dans la stratégie internationale de la France pour le numérique. Les membres de l'institut ont développé des partenariats notamment avec l'ANSSI, le SGDSN ou la CNIL. L'Institut participe aux grands débats relatifs à la cybersécurité en proposant son expertise dans de nombreux domaines.

Le Cluster EDEN

Le Cluster Eden né il ya 10 ans regroupe des entreprises françaises dédiées à la défense et à la sécurité. Ce cluster régional est devenu national.

Parmi les différentes entreprises du Cluster Eden, certaines sont spécialisées dans l'équipementier de protection personnelle ou de véhicules, d'autres dans la vidéo surveillance ou encore dans la cybersécurité.

Composé par près de 130 entreprises membres, dont la totalité sont des PME, ce cluster s'est affirmé en quelques mois comme l'un des groupes les plus importants des secteurs de la défense et de la sécurité.Bien qu'opérant dans toute la France, un quart de ces entreprises est basé dans la métropole de Lyon et la moitié en Auvergne-Rhône-Alpes. Le budget du cluster avoisine les 250 000 euros, il compte assurer le développement de ses activités en Europe.

On peut citer l'exemple d'Aleph Networks, start-up régionale aidée par le Cluster Eden. Parmi les entreprises du Cluster, Aleph Networks a la particularité d'être une start-up opérant pour la cybersécurité des particuliers et des professionnels.Créée en 2012 et animée par 7 salariés, cette entreprise travaille sur un sujet sensible : le développement d'un moteur de recherche, afin de lutter contre les hackers visant les réseaux sociaux des particuliers ou la base de données des entreprises et institutions. Il s'agit avant tout d'un système de surveillance et non d'anti-intrusion.

Les recommandations du CESER pour aller plus loin

Le CESER propose quelques recommandations à l'attention des acteurs régionaux pour faire de ce sujet un élément majeur et répondre aux défis qui l'accompagne. Il cible trois axes sur lesquels renforcer ou initier des actions Cela permettrait une meilleure appréhension du sujet sur le territoire et favoriserait le développement de la culture numérique. La cybersécurité est un volet nécessaire pour renforcer la confiance des acteurs et assurer la liberté numérique.

Les **trois axes** proposés sont :

AXE 1 → Poursuivre et accentuer la sensibilisation-formation des organisations et des individus, notamment les plus jeunes.

AXE 2 → Accompagner les organisations publiques, privées et associatives en portant une attention particulière aux petites structures qui sont souvent démunies face à ce défi.

AXE 3 → Fédérer les acteurs de la filière cybersécurité régionale et engager des coopérations à l'échelle nationale et européenne.

AXE 1

Poursuivre et accentuer la sensibilisation des organisations et des particuliers, notamment les plus jeunes

Le risque cyber est récent, à l'inverse d'autres risques, il ne fait pas l'objet sauf exception, d'une transmission dans les familles, dans les organisations, aussi il convient d'organiser l'information à travers des démarches proactives.

1

Le CESER propose de mettre en place des exercices de cybersécurité « proches » d'une attaque réelle (sur le modèle d'un exercice évacuation-incendie). Un logiciel de simulation pourrait être produit par les acteurs de la filière sous l'impulsion notamment du Conseil Régional à destination des organisations, voire des particuliers pour les sensibiliser en situation « réelle ».

2 Concernant les jeunes, une sensibilisation-formation à la cybersécurité et au traitement des informations (Fake-News) au titre de l'instruction civique pourrait être mise en place, puis au collège une formation spécifique sur la cybersécurité pourrait être intégré au B2I (Brevet informatique et internet) ou le compléter. Plus largement à chaque niveau pédagogique des temps consacrés à ce sujet et à ces évolutions très rapides pourraient intégrer les cursus pédagogiques. Dans la formation des futurs chefs d'entreprise, introduire un temps consacré à ce sujet et notamment leur faire connaître les réponses existantes serait pertinent. Ces démarches pourraient être menées par la Région en collaboration avec les acteurs concernés : rectorats, chambres consulaires …

3 La Région et ses partenaires privilégiés comme les quatre moteurs pourraient prendre une initiative à l'échelle européenne sur ce thème (livre blanc, manifeste.) pour inciter à une coopération renforcée. Une obligation d'information par les fournisseurs d'accès à Internet sur les attaques identifiées pourrait par exemple être suggérée.

4 Dans cette phase de sensibilisation, la société civile doit prendre sa part. La sensibilisation des citoyens passe également par le relai des organisations représentant la société civile. La société civile peut aussi agir dans la mobilisation pour une politique européenne plus affirmée sur le sujet. Le CESE européen pourrait se faire l'écho des attentes de la société civile européenne en la matière auprès du parlement européen.

AXE 2

Accompagner les organisations publiques, privées et associatives à se saisir de la question en portant une attention particulière aux petites structures qui sont souvent démunies face à ce défi

Les petites structures sont souvent les plus démunies face au défi de la cybersécurité. Ce thème doit être appréhendé de manière systémique. La sécurité est une chaîne qui concerne tous les acteurs. Une action volontariste de la collectivité régionale appuyée sur sa compétence en matière de développement économique et territorial serait pertinente. Certaines entités à l'échelon régional ont mis en place des plans spécifiques : grandes entreprises, collectivités et associations de taille importante. La Région pourrait s'appuyer sur celles-ci pour promouvoir un programme ambitieux sur ce sujet. Il s'agit notamment de prendre la question sous deux angles :

5 Un déploiement progressif mais rapide de plans d'actions au niveau des différentes organisations. Les têtes de réseau pourraient être mobilisées :

- Consulaires, organisations professionnelles pour les entreprises. Les grands donneurs d'ordre pourraient notamment davantage accompagner les entreprises sous-traitantes dans cette démarche, ils y ont intérêt si l'on considère les liens numériques entre elles dans les processus de production. La fraude aux fournisseurs est un bon exemple de liens exploités par les cyberdélinquants ;
- La Région et les grandes collectivités (métropoles, départements) dans l'appui aux petites collectivités ;
- Les têtes de réseau associatives pour les associations.

6 Un numéro vert, dont la Région pourrait assurer la maîtrise d'ouvrage, pour répondre aux situations d'urgence pourrait être expérimenté sur le territoire régional afin d'éviter la propagation de certaines attaques. Cela pourrait se faire en lien étroit avec les forces de police dont les moyens sont limités sur cette thématique.

AXE 3

Fédérer les acteurs de la cybersécurité régionale et engager des coopérations à l'échelle nationale et européenne

Le marché de la cybersécurité est un marché économique très porteur, des enjeux de souveraineté numérique y sont liés. Les enjeux de constitution d'une filière de la cybersécurité dépassent le strict cadre régional et s'inscrivent davantage dans des perspectives nationales et surtout européennes.

L'articulation de réponses en lien avec le développement de l'intelligence artificielle est déterminante.

Des initiatives en Région ont été lancées ou sont en cours de mise en œuvre. On peut citer le campus numérique, le cluster ECC4IU, le Grenoble Alpes Cyber Security Institute et l'existence de start-up largement identifiées sur ce thème mais aussi un écosystème de recherche et d'innovation particulièrement riches sur ces thématiques.

Sur ces sujets, le tissu industriel d'Auvergne-Rhône-Alpes constitue un terrain d'expérimentation particulièrement pertinent pour valoriser une démarche autour de la protection des systèmes industriels.

Le CESER propose que la Région fédère l'ensemble des initiatives sous une bannière commune, en organisant par exemple une journée rassemblant l'ensemble des acteurs régionaux concernés.
Elle pourrait notamment aussi inciter de grands acteurs du numérique en Région, tel Google par le biais des ateliers numériques initiés à Saint-Etienne, à engager également une action sur le thème de la cybersécurité. Parallèllement, des coopérations avec des régions ayant développées ces thématiques comme la Bretagne ou Région SUD Alpes Côte d'Azur pourront être mises en oeuvre La cybersécurité liée à l'internet des objets est un thème particulièrement porteur pour les régions industrielles comme Auvergne-Rhône-Alpes. Cet axe est complémentaire par ailleurs de la cybersécurité plus strictement orientée vers les réseaux informatiques qu'ont développé d'autres régions.

Conclusion

Garantir la sécurité de tout un ensemble d'échanges numériques est une condition nécessaire pour que l'ensemble des usagers, entreprises, administrations publiques, associations et particuliers se sentent en confiance dans leurs pratiques numériques et puissent ainsi les exercer librement et donc les développer.

Cette confiance passe par des actions que chacun des acteurs doit mettre en place pour garantir sa propre sécurité et celle de ceux qui sont en relation avec lui.

La surface d'exposition aux risques est croissante compte tenu de l'augmentation du nombre d'utilisateurs et des objets connectés, et la professionnalisation des fraudeurs. La cybersécurité relève de la sphère économique comme de la sphère politique car elle pose également des questions de souveraineté. Des actions ont été mises en œuvre au plan national et au plan régional. La Cybersécurité est également un marché en pleine croissance pour lequel des opportunités existent et les acteurs régionaux ne sont pas dépourvus d'atouts en la matière. Pour renforcer et développer la cybersécurité en Auvergne-Rhône-Alpes, territoire qui a fait du développement numérique une de ses priorités, le CESER propose aux acteurs régionaux trois axes d'actions : la sensibilisation-formation, notamment des plus jeunes, l'accompagnement des petites structures économiques, publics et associatives dans la mise en œuvre de couverture aux risques, et la réunion des initiatives sous une bannière commune pour y donner davantage de lisibilité. Les éléments relatifs aux besoins de compétences spécifiques à ce secteur et l'adaptation des formations, sont des points qui mériteraient un approfondissement rapide afin d'apporter des réponses opérationnelles aux acteurs. Face à ce nouveau défi qu'est la cybersécurité des réponses sont à construire, à inventer pour faire face à des actes malveillants qui évoluent très vite : leur pertinence sera la garantie de la confiance qui sera accordée aux actes numériques et donc à la liberté d'usage qui en découle.

Bibliographie

AGUILAR Eduardo, « Cluster Eden : des entreprises françaises de sécurité et défense en passe de devenir européennes », *Lyon Entreprises*, 23 novembre 2018. [en ligne] consulté le 8 janvier 2019. Disponible à l'adresse : <http://www.lyon-entreprises.com/News/L-article-du-jour/Cluster-Eden-i87521.html> .

BITTAN Michael et AKERMI Fouzi, *Enjeux cyber 2016*, Deloitte, 2016, 25 p.

CABINET EY, *Les formations et les compétences en France sur la cybersécurité*, OPIIEC, mai 2017, 124 p. [en ligne] consulté le 8 janvier 2019. Disponible à l'adresse : <https://www.fafiec.fr/images/contenu/menuhaut/observatoire/etudes/2017/cybers%C3%A9curit%C3%A9/21-05-2017_Etude_cybersecurite_rapport.pdf>

CISCO, *Cisco 2018 : Rapport annuel sur la cybersécurité*, CISCO, février 2018, 67 p.

CISCO, *Rapport annuel 2017 sur la cybersécurité*, CISCO, janvier 2017, 109 p.

DELISLE Corinne, « Lyon place forte de la cybersécurité », *Bref Eco Auvergne-Rhône-Alpes*, 6 février 2018. [en ligne] consulté le 8 janvier 2019. Disponible à l'adresse : <http://www.brefeco.com/actualite/logiciels-services-numeriques/lyon-place-forte-de-la-cybersecurite>

EULER HERMES, « Etude Fraude 2018 : face à des fraudeurs de plus en plus professionnels, les entreprises restent insuffisamment armées », 10 avril 2018. [en ligne] consulté le 8 janvier 2019. Disponible à l'adresse : <http://www.eulerhermes.fr/mediacenter/actualites/Pages/etude-fraude-2018.aspx>

GATEAUD Pascal et MORAGUES Manuel, « Le RGPD est un texte historique », *L'Usine nouvelle*, 15 avril 2018, pp. 44-45

LAHOUD Marwan, *Cybermenace : avis de tempête*, Institut Montaigne, novembre 2018, rapport 107 p. et synthèse 2 p. [en ligne] consulté le 8 janvier 2019. Disponible à l'adresse : <https://www.institutmontaigne.org/publications/cybermenace-avis-de-tempete>

MEDDAH Hassan, « La cybersécurité imposée à tous », *L'Usine nouvelle*, 15 avril 2018, pp. 34-35

MEDEF, « Evaluez votre niveau de connaissance sur le RGPD grâce au MEDEF ! », 2018. [en ligne] consulté le 8 janvier 2019. Disponible à l'adresse : <https://rgpd.medef.com/>

« De belles perspectives pour Cybelius dans la cybersécurité », *Bref Eco Auvergne-Rhône-Alpes*, 28 mars 2018

Données personnelles et RGPD : comment faire ?, Confédération des PME (CPME), mars 2018, 16 p. [en ligne] consulté le 8 janvier 2019. Disponible à l'adresse : <https://www.cpme.fr/upload/ftp/rgpd-comment-faire-180326.pdf>

« Collectivités et industriels en quête de cybersécurité », *Le Progrès*, février 2018

« Sentryo, la vigie des systèmes industriels », *Le Progrès*, 9 décembre 2017

« Schneider Electric et le Lyonnais Sentryo unissent leurs forces », *Le Progrès*, 11 octobre 2017

« Sentryo élue entreprise de cybersécurité de l'année au Canada », *Le Progrès*, 6 juin 2017

« Flash spécial Cyber Sécurité », *UNAPL*, 17 mai 2017[en ligne] consulté le 8 janvier 2019. Disponible à l'adresse : <http://www.unapl.fr/espace-presse/communiques/flash-special-cyber-securite>

Cybersécurité ce qu'il faut faire pour se protéger, UNAPL, mai 2017, 21 p.

Université Grenoble Alpes « Cybersecurity Institute : remodeler technologies et sciences sociales »

Déclarations des groupes

Intervention de Mme Delphine ROUSSY, au nom des organisations CFDT, CFE-CGC, CFTC, CGT, FSU, Solidaires et UNSA (Collège 2)

La commission 1 a choisi de travailler en 2018 sur le thème de la cybersécurité, et la note d'alerte qui a été produite justifie en elle-même la pertinence de notre assemblée sur ce sujet.

En effet, comme indiqué dans la note, la cybersécurité est désormais l'affaire de chacun, que ce soit dans les entreprises, dans les collectivités, les administrations, mais également dans l'ensemble des organisations de la société civile que nous représentons ici. Il est aussi indispensable de sensibiliser et de mobiliser plus largement les citoyens.

La commission a auditionné de nombreux témoins qui ont tous convergé vers un même constat que nous partageons : la sécurité des systèmes d'information et des données est un enjeu majeur non pas pour notre avenir, mais déjà dans notre quotidien.

Sans répéter les éléments de la note, nous souhaitons insister sur quelques points en particulier.

Tout d'abord, le rôle de la formation professionnelle : garantir la sécurité des systèmes d'information est un challenge, mais représente aussi une formidable opportunité pour l'emploi, si tant est que les salariés soient correctement formés. Nous estimons qu'il y a de vrais parcours de formation à construire, à coordonner, à financer, et la Région doit prendre toute sa place dans ce processus. Nous craignons malheureusement que le désengagement de la Région en la matière, déjà évoqué lors de la discussion sur le BP en décembre dernier, ne permette pas de débloquer les crédits nécessaires à l'accompagnement de l'évolution des emplois et compétences.

Un autre aspect concerne les enjeux de sensibilisation et de prévention des risques liés au cyberharcèlement sous ses différentes formes. Cela concerne tant le cadre de la vie « personnelle et familiale », avec une attention particulière au milieu scolaire, mais aussi celui de la vie « professionnelle » avec la nécessité de formaliser de nouveaux droits, notamment le droit à la déconnexion et le droit à l'oubli.

Un autre enjeu crucial pointé concerne la situation des « petites » organisations. En effet, même si toute organisation peut être mise en difficulté par des attaques informatiques, force est de constater que les grandes entreprises et les grosses collectivités, sont toutes en train de s'organiser, en s'appuyant sur des services informatiques souvent déjà existants, pour répondre à cette menace. Mais qu'en sera-t-il des PME et TPE, des collectivités locales de plus petite taille ? Elles n'ont ni les compétences ni les moyens pour se préparer ; face à un tel constat des initiatives sont prises par différents acteurs : représentants professionnels, chambres consulaires…

Nous pensons également que l'on doit avoir un focus particulier sur le secteur de l'économie sociale et solidaire et l'ensemble du monde associatif, en dehors de quelques grandes structures, et qui ne disposent pas des structures professionnelles collectives mentionnées ci-dessus. Des soutiens particuliers doivent pouvoir leur être attribués avec un focus particulier sur la formation de leurs salariés et de leurs nombreux bénévoles.

Là encore, nous pensons que la Région, en tant que collectivité majeure, doit pouvoir jouer un rôle de tête de pont, comme mentionné par la note.

La Région pourrait également servir de leader dans un domaine crucial qu'est celui du stockage des données. En effet, pour assurer la sécurité des données-tant en termes de conservation que d'usages, il est utile d'envisager des stockages en France ou en Europe. Notre région pourrait se positionner sur ce nouveau créneau de développement économique.

Enfin, nous souhaitons nous attarder sur les conséquences de ces nouvelles menaces pour les salariés des entreprises. En effet, certains attaquants visent des salariés pour atteindre, à travers eux, l'entreprise qui les emploie. Ces attaques utilisent la plupart du temps des informations de la sphère privée des salariés, par exemple sur les réseaux sociaux. A l'heure où certaines entreprises prônent le « PAP (Prenez vos Appareils Personnels), quelle sera la faute d'un salarié s'il s'avère qu'il est devenu la « porte d'entrée » pour une attaque contre son employeur ? Un salarié sera-t-il responsable si son appareil personnel n'est pas à jour sur les outils de sécurité ? Nous pensons que les entreprises et les organisations syndicales de salariés doivent se saisir de ce sujet en amont, pour sensibiliser et prévenir sans attendre. En cela, cette note pourra servir de base et de boîte à outils.

Enfin pour conclure, la division du travail et le recours toujours plus grands, aujourd'hui à la sous-traitance et demain au travail collaboratif, nécessiteront une vigilance renforcée sur les conditions économiques et sociales réellement exercées. Nous pensons que le renforcement du dialogue social dans et autour du périmètre social de l'entreprise permet d'apporter des réponses et de limiter les risques pour les entreprises et les salariés.

Pour toutes ces raisons, nous voterons la note présentée par la commission 1.

Intervention de Mme Aurélie DESSEIN, au nom descollèges 3 et 4

Monsieur le Président, Mesdames les conseillères, Messieurs les conseillers,

Qu'elle soit gage de progrès, de développement de l'économie, d'évolution technologique ou même, comme de nombreux usagers peuvent le redouter lorsque l'isolement humain s'accentue, de recherche d'économie de moyens, l'ère du numérique s'impose dans le quotidien de chacun. Parallèlement, les enjeux de la sécurité numérique évoluent rapidement et comme le soulignait le CESE européen dans ses récents travaux, si l'on veut faire de la cybersécurité une réalité, l'implication de tout un chacun s'avère nécessaire et le rôle des autorités régionales ne doit pas être négligé.

Dans l'optique de développer la culture commune sur ce sujet, le présent rapport expose, de façon pratique, les principales expositions aux risques, depuis les organisations jusqu'aux citoyens, et les sources d'informations ou de réponses opérationnelles. L'intérêt des recommandations qui y sont présentées est à souligner.

En complément, les collèges 3 et 4 souhaitent mettre l'accent sur les points de vigilance suivants.

L'ANSII (Agence nationale de la sécurité des systèmes d'informations) souligne que majoritairement, la sécurité du numérique repose sur des mesures simples et des bonnes pratiques à adopter dans la sphère privée et professionnelle. Le facteur humain est l'une des principales causes des accidents de cybersécurité. Il est donc nécessaire d'établir une solide base de cyber-compétences et d'améliorer la cyber-hygiène et la sensibilisation auprès des particuliers et des entreprises.

Or, le numérique s'immisce de plus en plus tôt dans la vie de chacun. De la même manière que l'éducation inculque progressivement aux jeunes enfants les outils pour parer aux risques (physiques, relationnels, etc) auxquels ils sont confrontés dans leur évolution, des modules d'information sur la sécurité numérique, adaptés à chaque âge de la vie, méritent d'être proposés de l'enfance jusqu'à un âge adulte avancé, voire très avancé.

Le CESE est lui-même favorable à la mise en place d'un programme de formation certifié par l'UE à l'intention des établissements du second degré et des professionnels.

Différents acteurs peuvent intervenir dans cette perspective. Pour la Région AuRA, l'information et la formation à la cybersécurité méritent d'être intégrées à la politique relative au développement du numérique qu'elle soutient avec ambition. Ainsi, proposer aux lycéens et aux étudiants des modules sur les précautions élémentaires telles celles recommandées par l'ANSII s'avérerait judicieux et précurseur.

Proposer cette information aux habitants, ainsi qu'aux associations et petites structures professionnelles s'avèrera tout aussi opérant. Pour ce faire, les bons acteurs doivent être formés, accompagner la démarche.

Parallèlement, dans l'objectif de développer les métiers d'avenir, l'ambition de faire connaître les possibilités de débouchés dans le domaine de la cybersécurité, et le développement de la formation aux métiers en lien avec la sécurité numérique méritent particulièrement le soutien des acteurs régionaux.

Le lieu de stockage, en lui-même, de ces données constitue lui aussi un enjeu considérable étant donné le contexte législatif variable d'un pays à un autre. En ce qui concerne les données privées collectées par les organismes publics ou assimilés, le stockage en local mérite là-aussi d'être favorisé et maîtrisé.

Les collèges 3 et 4 souhaitent en outre attirer l'attention sur des préoccupations des citoyens en termes de sécurité numérique, de droit à l'oubli et de droit à l'anonymat. Des objets connectés s'imposent dans le quotidien de chacun et accentuent les inquiétudes.

Pour exemple, le compteur communicant Linky, installé dans tous les foyers français d'ici 2021 n'en finit pas de créer des suspicions : n'est-il pas une cible parfaite en termes d'exploitation des données de façon non consentie par les usagers ?

Autre exemple souvent évoqué, l'installation accrue, dans les zones publiques, de caméras ; qui outre le sentiment de sécurité relative qu'elles peuvent ponctuellement apporter, génèrent aussi une gêne en termes de liberté individuelle et de questionnements quant aux usages qui peuvent dériver. Les maires et les élus régionaux ont un rôle majeur dans ces choix d'aménagement du territoire.

Aussi face à ces questionnements, les pouvoirs publics se doivent-ils d'apporter à la population des preuves régulières du contrôle accru du respect des lois de confidentialité et encadrer l'emprise des préoccupations économiques ou de surveillance, par une défense objective des règles de libertés individuelles.

Ainsi, parallèlement aux recommandations relatives à la prévention des cyberattaques et de la cybercriminalité proposées dans le présent rapport, une grande vigilance quant aux incidences de la généralisation du numérique semble nécessaire pour garantir un niveau de sécurité important des populations.

Les collèges 3 et 4 voteront cet avis.

Contributeurs

Éric LE JAOUEN
Président de la Commission 1 « Activités économiques, emploi et innovation »
Collège 1

Michel-Louis PROST, 2ème Vice-Président, Référent de la commission

Jean-Marc GUILHOT, Vice-Président délégué, Président de la conférence des présidents

COLLÈGE 1*

BERNELIN Thierry (UDES)
BLANC Dominique (UNAPL-CNPL)
BREUIL Irène (CCIR)
CABUT Bruno (U2P)
CELMA Patrick (MEDEF)
CHABBAL Jean (Pôle de compétitivité)
CHARVERON Philippe (MEDEF)
DUPLAIN Jocelyne (CCIR)
FLAUGÈRE Jean-Luc (CRA)
MARTEL Alain (Pôle de compétitivité)
SIQUIER Marie-Amandine (CCIR)
TARLIER Bruno (CPME)
TRICHARD Alain (ARIA)
VAYLET Jean (CCIR)

COLLÈGE 2*

ACOLATSE Erick (CFE-CGC)
BASCOULERGUE Gisèle (CGT)
BOLF Édith (CFDT)
BOUVIER Bruno (CGT)
CARCELES Robert (CFE-CGC)
COHEN-ALORO Fabien (UNSA)
DELAUME Colette (FO)
FATIGA Antoine (CGT)
FAURE Philippe (CGT)
JUYAUX Christian (CFDT)
LAURENT Bernard (CFTC)
PICHOT Arnaud (FO)
PUTOUX Laurent (CGT)
ROUSSY Delphine (CFDT)
VINCIGUERRA Pio (FO)

COLLÈGES 3 et 4*

BABOLAT Guy (UR SCOP)
BAREAU Anne-Marie (Filière Bois)
BONNEFOY Thomas (JCE)
CLAVERANNE Jean-Pierre (CREAI)
CONDAMIN Yvon (MRIE)
DESSEIN Aurélie (PQ Environnement)
FAUREAU Bernard (PQ)
GELAS Nadine (PQ)
JUILLAND Christine (Habitat)
MARGUIN Christophe (PQ)
PAIX Stéphanie (PQ)
POSSE Robert (UFC Que Choisir)
ROSENBERG Armand (CRESS)
VIAL-VOIRON Victor-John (UNPI)
VIGNAT Josette (CRT)

Remerciements

Personnes auditionnées

2 mai 2018	Services de l'État
4 juillet 2018	**MIS Jean-Michel**, Député de la Loire
5 septembre 2018	**DRAPEAU Christelle**, Coordinatrice du Cluster Européen ECC4iu **MATHIEU Jean-Christophe**, Président du Cluster Européen ECC4iu (European Cybersecurity Cluster for Industrials and Urbans Systems) et Responsable de la Sécurité des Produits et Solutions pour Siemens France
7 novembre 2018	**DARRIGOL Jean-Marc,** Directeur des Systèmes d'Information et des Usages Digitaux au Conseil régional Auvergne-Rhône-Alpes **DUSSAIX Philippe,** Délégué Général à la Sécurité au Conseil régional Auvergne-Rhône-Alpes **NEUMAYER Mathieu,** Responsable de la Sécurité des Systèmes d'Information au Conseil régional Auvergne-Rhône-Alpes

Contacts

Laurent DE PESSEMIER
Chargé d'études
Tél. : 04.26.73.40.08
laurent.depessemier@auvergnerhonealpes.fr

Informations

Vous souhaitez suivre l'actualité du

CESER Auvergne-Rhône-Alpes, inscrivez-vous à la lettre.ceser@auvergnerhonealpes.fr

ou

retrouvez les informations sur

le site internet de la Région Auvergne-Rhône-Alpes :

www.auvergnerhonealpes.fr/ceser

La cybersécurité est porteuse de nombreux enjeux : captations d'informations, surveillance de sites visités, intégrité des données stockées, détournement de flux financiers, piratage, usurpation d'identités …

Cette note de sensibilisation, sur le sujet, a pour objet d'attirer l'attention des acteurs régionaux sur le thème et d'insister sur le fait que la cybersécurité est l'affaire de tous.

Après avoir montré que la surface d'exposition aux risques est croissante, le CESER pointe que les enjeux sont politiques et économiques, il présente également les initiatives prises tant au plan national que régional.

Enfin, il propose des recommandations aux acteurs régionaux pour mobiliser davantage sur ce thème.

NUMERIQUE • CYBERSÉCURITÉ • SÉCURITÉ INFORMATIQUE
RGPD • INTELLIGENCE ÉCONOMIQUE • CYBERCRIMINALITÉ
CONFIANCE NUMÉRIQUE • ENTREPRISE
EUROPE : POLITIQUE ÉTRANGERE ET DE SÉCURITÉ COMMUNE
AUVERGNE-RHONE-ALPES

www.auvergnerhonealpes.fr/ceser

Crédit photos : 123 RF
istockphoto

Note

CESER Auvergne - Rhône-Alpes / Lyon
8 rue Paul Montrochet – CS 90051 – 69285 Lyon cedex 02
T. 04 26 73 49 73 – F. 04 26 73 51 98

CESER Auvergne - Rhône-Alpes / Clermont-Ferrand
59 Bd Léon Jouhaux – CS 90706 - 63050 Clermont-Ferrand Cedex 2
T. 04.73.29.45.29 – F. 04.73.29.45.20