CESER

Région îledeFrance

avis & rapport

Cyberprévention : un enjeu de sécurité et de citoyenneté pour tous en Île-de-France

12 déc. 2023

Rapport et avis présentés au nom de la commission Développement économique
par **Bernard COHEN-HADAD** et **Vincent GAUTHERON**

CESER Région îledeFrance

avis

Avis n°2023-23
présenté au nom de la commission Développement économique
par **Bernard COHEN-HADAD** et **Vincent GAUTHERON**

Cyberprévention : un enjeu de sécurité et de citoyenneté pour tous en Île-de-France

12 déc. 2023

Avis n° 2023-23
présenté au nom de la commission Développement économique
par **Bernard COHEN-HADAD** et **Vincent GAUTHERON**

12 décembre 2023

Cyberprévention : un enjeu de sécurité et de citoyenneté pour tous en Île-de-France

Certifié conforme

Le président

Éric BERGER

Le Conseil économique, social et environnemental régional d'Île-de-France

Vu :

- Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOUE du 4 mai 2016 ;
- Le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'Agence de l'Union européenne pour la cybersécurité et à la certification de cybersécurité des technologies de l'information et des communications, JOUE du 7 juin 2019 ;
- Le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données*,* JOUE du 3 juin 2022 ;
- Le règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, JOUE du 14 septembre 2022 ;
- Le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques, JOUE du 27 octobre 2022 ;
- Le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, JOUE du 27 décembre 2022 ;
- La directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, JOUE du 27 décembre 2022 ;
- Le code général des collectivités territoriales et notamment l'art. L4221-1 relatif aux compétences du Conseil régional et l'art. L4241-1 relatif aux missions du Conseil économique, social et environnemental régional auprès du Conseil régional ;
- Le code des assurances, Livre I^{er} : *Le contrat*, Titre II : *Règles relatives aux assurances de dommages*, Chapitre X : *L'assurance des risques de cyberattaques*, art. L12-10-1 ;
- Le code de la consommation, Livre I^{er} : *Information des consommateurs et pratiques commerciales,* Titre I^{er} : *Information des consommateurs*, Chapitre I^{er} : *Obligation générale d'information précontractuelle*, art. L111-7-3 ;
- Le code monétaire et financier, Livre I^{er} : *La monnaie*, Titre VI : *Dispositions pénales*, Chapitre III : *Infractions relatives aux chèques et aux autres instruments de la monnaie scripturale* (art. L163-1 à L163-12) ; Livre V : *Les prestataires de services*, Titre VII : *Dispositions pénales*, Chapitre I^{er} : *Dispositions relatives aux prestataires de services bancaires* (art. L571-1 à L571-16) ;
- Le code pénal, Livre III : *Des crimes et délits contre les biens*, Titre II : *Des autres atteintes aux biens*, Chapitre III : *Des atteintes aux systèmes de traitement automatisé de données,* art. 323-1 à 323-8 ;
- La loi n^{o} 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978 ;
- La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF du 22 juin 2004 ;
- La loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF du 19 décembre 2013 ;
- La loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, JORF du 14 juillet 2018 ;
- La loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur, JORF du 25 janvier 2023 ;
- Le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé Agence nationale de la sécurité des systèmes d'information, JORF du 8 juillet 2009 *(modifié par décrets successifs)* ;

- L'arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance, JORF du 5 mars 2017 *(modifié par arrêtés successifs)* ;
- La délibération n° CP 2022-123 : *Filière cybersécurité*, adoptée par la commission permanente du Conseil régional d'Île-de-France le 23 mars 2022, qui autorise la signature de la convention de partenariat entre la Région Île-de-France et l'Autorité nationale de sécurité des systèmes d'information, complétée par la délibération n° CP 2022-483 adoptée par la commission permanente le 19 novembre 2022 : *CERT régional, grands lieux d'innovation, pack quantique* ;
- La délibération n° CR 2022-029 : *Schéma régional de développement économique d'innovation et d'internationalisation (SRDEII) 2022-2028*, adoptée par le Conseil régional d'Île-de-France le 19 mai 2022 ;
- La délibération n° CR 2023-018 *: Budget supplémentaire 2023*, adoptée par le Conseil régional d'Île-de-France le 31 mai 2023, qui attribue un budget sur le nouveau dispositif « Chèque Cyber » ;
- La délibération n° CP 2023-246 : *Tiers-lieux et autres affaires économiques*, adoptée par la commission permanente du Conseil régional d'Île-de-France le 5 juillet 2023, qui modifie le règlement d'intervention relatif aux « Chèques en faveur de la transition numérique et écologique des artisans et commerçants franciliens » ;
- La délibération n° CP 2023-327 : *Filières et innovation*, adoptée par la commission permanente du Conseil régional d'Île-de-France le 21 septembre 2023, qui crée le dispositif « Chèque Cyber » et en adopte le règlement d'intervention ;
- La délibération n° CR 2023-052 : *Orientations budgétaires pour 2024*, adopté par le Conseil régional d'Île-de-France le 16 novembre 2023 ;
- La délibération n° CR 2023-381 : *Filières et innovation*, adoptée par la commission permanente du Conseil régional d'Île-de-France le 17 novembre 2023 ;
- L'avis d'attribution de marché public n° 23-94497 *: Prestations de déploiement du CSIRT de la Région Île-de-France - Lots 1 à 3*, BOAMP du 7 juillet 2023 ;
- L'appel à manifestation d'intérêt : *Référencement de prestataires cybersécurité (niveau 2) franciliens par le CSIRT Île-de-France,* publié sur le site internet de la Région Île-de-France (consulté le 26 octobre 2023) ;
- Le rapport et l'avis du Conseil économique, social et environnemental régional d'Île-de-France n°2020-15 du 15 octobre 2020 : *L'Entreprise 4.0 : réussir le passage à l'entreprise du futur* (Clément DE SOUZA) ;
- L'avis du Conseil économique, social et environnemental n°2022-007 du 13 avril 2022 : *Climat, cyber, pandémie : le système assurantiel mis au défi des risques systémiques* ;
- L'avis du Conseil économique, social et environnemental régional d'Île-de-France n° 2022-04 du 12 mai 2022 : *Schéma régional de développement économique, d'innovation et d'internationalisation (SRDEII) 2022-2028* (Vincent PIGACHE) ;

Considérant :

- **L'accélération de la transformation numérique,** à la faveur d'un taux d'équipement élevé des particuliers (plus de neuf Français sur dix sont aujourd'hui connectés[1]) et d'un intérêt croissant des entreprises pour le numérique, en particulier les très petites et moyennes entreprises (TPE et PME) dont la présence en ligne ne cesse de progresser (84 % d'entre elles déclarent disposer d'au moins une solution de visibilité en ligne[2]) ;

- **Le niveau élevé de la cybermenace,** dans un contexte géopolitique sensible qui accroît l'exposition au risque numérique des entreprises comme des particuliers ;

[1] *Baromètre du numérique 2022*, enquête réalisée par le ministère délégué chargé de la Transition numérique et des télécommunications avec l'ARCEP, l'ARCOM, l'ANCT et le Conseil général de l'économie, janvier 2023.
[2] *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023*, étude réalisée pour FranceNum par le Centre de recherche pour l'étude et l'observation des conditions de vie (CRÉDOC), septembre 2023.

- **Les risques supplémentaires propres au territoire francilien,** qui concentre un grand nombre de centres décisionnels, de sièges sociaux, d'organismes de recherche etc. et dont la qualité de terre d'accueil de grands évènements internationaux (Coupe du monde de rugby 2023, Jeux Olympiques et Paralympiques 2024) renforce encore l'exposition aux attaques des systèmes d'informations des opérateurs et acteurs économiques nationaux et régionaux ;

- **Le déport progressif des cyberattaques vers les TPE, PME et les entreprises de taille intermédiaire (ETI)** (40 % des rançongiciels rapportés à l'Autorité nationale de sécurité des systèmes d'information (ANSSI) en 2022[3]), **les collectivités territoriales** (23 %), **les établissements publics de santé** (10 %) **et les associations** (6 %), moins protégés que les grands organismes publics et les grandes entreprises ;

- **Les vulnérabilités particulières des TPE et PME exploitées par les cybercriminels** : un niveau de sécurité insuffisant, des ressources humaines et financières limitées, une offre de service peu lisible et insuffisamment adaptée – voire le sentiment que son activité n'est pas concernée : pourtant, *« au cours des trois dernières années, le nombre d'entreprises de moins de dix salariés (TPE) ayant subi une attaque* [dans le monde] *a augmenté de plus de moitié pour atteindre 36 % »*[4] *;*

- **Les enjeux d'adaptation des entreprises aux nouvelles pratiques de la consommation :** la numérisation d'un nombre croissant de procédures, la mise en place de la facturation électronique obligatoire, le développement du paiement sans-contact peuvent constituer des sources d'inquiétude pour de nombreux chefs d'entreprise, particulièrement des TPE-PME ;

- **Le développement du *flex-office*, du télétravail ou du travail en tiers-lieu**, qui rend plus difficile la sécurisation de l'accès aux données de l'entreprise, particulièrement marqué en Île-de-France : 45 % des actifs franciliens travaillent à distance (20 % avant la pandémie de la Covid-19 ; 34 % en moyenne nationale[5]), en moyenne 2,1 jours par semaine[6] et plus en période d'accueil de grands évènements ;

- **La nécessaire prise en compte du facteur humain,** au-delà des enjeux techniques : alors que les techniques de fraude par ingénierie sociale se perfectionnent (74 % des cyberattaques réussies contre une entreprise exploitent des imprudences ou un défaut de vigilance de la part d'un collaborateur[7]), ce qui appelle des actions nouvelles de sensibilisation, de formation professionnelle et de dialogue social de la part des employeurs publics et privés ;

- **Les risques multiples qu'encourent les entreprises victimes de cyberattaque :** les pertes financières directes (frais d'investigation et de remédiation des systèmes d'information concernés, transactions frauduleuses) et indirectes (interruption d'activité, perte de chiffre d'affaires à la suite de ventes non réalisées), l'atteinte à l'image et à la réputation de l'entreprise, la perte de données et le risque juridique (pénalités contractuelles, responsabilité civile et pénale) peuvent conduire une entreprise à disparaître, notamment les plus fragiles : plus d'une TPE-PME sur deux – selon les études disponibles, jusqu'à trois sur quatre – déposerait le bilan dans les trois ans qui suivent une cyberattaque réussie ;

- **Une prise de conscience encore insuffisante des chefs d'entreprise, notamment des plus petites :** 48 % des dirigeants de TPE-PME seulement expriment des craintes relatives à la sécurité des données de leur entreprise[8] ;

---

[3] *Panorama de la cybermenace 2022*, Agence nationale de la sécurité des systèmes d'information, janvier 2023.
[4] *Rapport Hiscox 2023 sur la gestion des cyber-risques – 7ème édition*, étude réalisée pour Hiscox Assurances par Forrester Consulting, octobre 2023.
[5] Norme Ifop de climat social, enquête menée en octobre 2022 auprès d'un échantillon représentatif de 1300 salariés, citée par *Le Journal du Dimanche*, Télétravail : l'Île-de-France championne du travail à distance, publié le 21 janvier 2023.
[6] *Baromètre des Franciliens – Édition 2023*, enquête réalisée pour l'Institut Paris Région par Ipsos, octobre 2023.
[7] *Baromètre annuel de la cybersécurité des entreprises – 8ème édition*, enquête réalisée pour le Club des experts de la sécurité de l'information et du numérique (CESIN) par OpinionWay, janvier 2023.
[8] *Le numérique dans les TPE et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023*, FranceNum / CRÉDOC, op. cit.

- **L'engagement croissant de l'État, des autorités publiques et des grandes collectivités territoriales, en particulier les régions,** pour encourager le développement de solutions pour les chefs d'entreprise, les responsables associatifs, les élus locaux et agents de la fonction publique ;

Émet l'avis suivant :

Le risque numérique n'est pas une fatalité : s'il n'épargne plus personne (États, administrations, collectivités, établissements publics, entreprises, associations, personnalités et citoyens), des solutions existent pour s'en protéger.

Pourtant, on constate peu d'engagement opérationnel des entreprises, notamment les TPE-PME, comme des associations et des petites collectivités territoriales : la cyberprévention, condition essentielle de la cybersécurité et de la résilience du territoire francilien – dont l'exposition aux cyberattaques est particulièrement élevée – présuppose la prise de conscience de la réalité du risque numérique. Or, les enquêtes s'accordent sur le fait que cette prise de conscience est encore insuffisante.

Par ses compétences et le rôle qu'elle joue sur le territoire, en particulier pour les entreprises dont elle est une interlocutrice privilégiée, la Région Île-de-France est légitime à agir. Engagée dans un processus interne de transformation numérique, elle a par ailleurs fait de la *« défense de la souveraineté industrielle et numérique »* l'un des axes stratégiques de son Schéma régional de développement économique, d'innovation et d'internationalisation (SRDEII) 2022-2028[9], dont les premières réalisations dans le champ de la cybersécurité se sont engagées à la rentrée 2023.

Ces initiatives sont récentes et il est bien trop tôt pour en évaluer la pertinence et l'efficience. Les propositions qui suivent se veulent une contribution positive et attentive du Ceser Île-de-France à une nouvelle politique publique régionale qui trouvera sa pleine maturité en s'inscrivant dans la durée et en s'adaptant à la diversité des acteurs concernés sur le territoire francilien.

Condition pour transformer les risques et défis en atouts pour le territoire francilien, **la cyberprévention est une responsabilité collective ; elle constitue en cela un enjeu de sécurité et de citoyenneté.**

Titre I^er^ – Accélérer la sécurisation numérique du territoire francilien

Article 1 : Fondre le Chèque Cyber et le Chèque numérique en une nouvelle aide unique

Le Ceser prend acte de la création par le Conseil régional d'un « Chèque Cyber[10] » en deux volets :

- Une première aide pour identifier, via un diagnostic effectué par un expert labellisé, les vulnérabilités des systèmes d'information des entreprises éligibles ;
- Une seconde aide, conditionnée à la réalisation d'un diagnostic, destinée à soutenir les dépenses d'investissement pour augmenter leur niveau de protection.

Le choix du Conseil régional de conditionner le versement de l'aide au diagnostic au recours à un prestataire dont le siège est situé en Île-de-France paraît pertinent pour renforcer l'écosystème cyber francilien. Par ailleurs, le dispositif répond aux difficultés, exprimées par les entreprises, d'une offre de service des prestataires en sécurité informatique encore trop peu lisible sur le territoire francilien, en les amenant à retenir des solutions d'équipement sur la base d'un diagnostic conduit par un professionnel sourcé et labellisé. En cela, il participe à une nouvelle politique publique de prévention du risque numérique.

[9] Délibération n° CR 2022-029 : *Schéma régional de développement économique d'innovation et d'internationalisation (SRDEII) 2022-2028*, adoptée par le Conseil régional le 19 mai 2022.
[10] Délibération n° CP 2023-327 *: Filières et innovation,* adoptée par la commission permanente du Conseil régional le 21 septembre 2023.

Attentif à la situation des petites structures et à l'adaptation des aides à la réalité du tissu économique francilien, le Ceser regrette pourtant que le règlement d'intervention de ces deux nouvelles aides cible exclusivement les PME (plus de dix salariés). **Cette approche amène à exclure de ce dispositif les TPE, qui représentent 78,5 % des entreprises franciliennes[11], ainsi qu'un grand nombre d'associations.** Ces deux catégories de structures n'échappent pourtant plus au risque de cyberattaque, ce qui présente des risques pour leur activité, comme pour celles de leurs partenaires, client et prestataires, si elles ne sont pas en mesure de rehausser leur niveau de sécurité numérique.

C'est pourquoi le Ceser propose de **fondre le « Chèque Cyber » et le « Chèque numérique[12] » en une nouvelle aide unique :**

- **Associant accompagnement à la transition et à la sécurisation numérique,** qui ne peuvent pas être envisagées séparément ;
- **Accessible à une plus grande diversité** de structures éligibles en taille comme en secteurs d'activité (incluant les entreprises de service par exemple) ;
- **Dans une approche élargie du type de dépenses éligibles à l'aide régionale :** la nouvelle aide unifiée pourrait aussi prendre en compte l'achat de licences de solutions informatiques de protection, les frais d'assurance contre le risque cyber, ou bien encore les dépenses d'assistance à maîtrise d'ouvrage pour l'implémentation de solutions sur la base des résultats du diagnostic de sécurité numérique.

Cette recommandation prolonge la proposition exprimée par le Ceser dans son avis relatif au SRDEII 2022-2028[13].

Dans le même esprit, le Ceser souhaite que **les prestations d'urgence du centre régional de réponse aux incidents cyber (CSIRT) « UrgenceCyber Île-de-France »,** dont le cahier des charges[14] précise qu'il ne concerne que les PME, les ETI, les associations nationales, les collectivités territoriales et leurs établissements publics**, puissent être ouvertes aux TPE et aux associations locales,** afin d'offrir un premier niveau de réponse à tous les acteurs concernés par le risque numérique.

Article 2 : Accélérer la sécurisation des réseaux wifi publics

Dans le prolongement de la participation de la Région Île-de-France au déploiement du « très haut-débit » sur le territoire régional, et dans un contexte de développement massif des téléservices, **le Ceser recommande à la Région d'accélérer la sécurisation des réseaux wifi publics,** source avérée de cyberattaques, **au sein des établissements qu'elle finance directement ou indirectement ou de ceux qui agissent par délégation** (lycées publics, universités et espaces de travail des étudiants, gares du réseau Île-de-France Mobilités, etc.).

[11] *Chiffres-clés de la région Île-de-France 2023*, L'Institut Paris Région avec l'INSEE et la Chambre de commerce et d'industrie Paris Île-de-France, juin 2023.
[12] Délibération n° CP 2023-246 : *Tiers-lieux et autres affaires économiques*, adoptée par la commission permanente du Conseil régional le 5 juillet 2023.
[13] Avis du Ceser Île-de-France n° 2022-04 du 12 mai 2022 : *SRDEII 2022-2028,* article 12 : *« Le Ceser observe l'effort mis en place par la Région pour accompagner de manière spécifique les différents types d'entreprises dans leur transition numérique. […] Néanmoins, la Région doit veiller à s'assurer des objectifs atteints en matière de transition numérique fondamentale pour l'ensemble des acteurs de l'écosystème francilien sous le prisme de la réduction des inégalités territoriales. […] Ainsi, une évaluation des capacités digitales des TPE, PME et ETI pourraient être menées dans la continuité de la généralisation des aides comme celle du "Chèque numérique". »*
[14] Délibération n° CP 2022-123 : *Filière cybersécurité,* adoptée par la commission permanente du Conseil régional le 23 mars 2022.

Titre II : Sensibiliser tous les Franciliens au risque numérique et aux moyens de s'en protéger

Article 3 : Diffuser les bonnes pratiques d'hygiène numérique au plus grand nombre

Pour le Ceser, la signature par la Région Île-de-France, en octobre 2023, de la *CharteCyber*[15] proposée par CyberMalveillance, le service public d'information, de prévention et de réaction aux cyberattaques, s'inscrit dans la volonté de sensibiliser le plus large public à ces problématiques. Ce faisant, la Région s'est engagée à *« démontrer l'importance de la cybersécurité [en son sein], en témoigner auprès de [son] écosystème et encourager toutes les autres organisations à adopter cette démarche ».*

Pour accompagner le développement du « réflexe cyber » auprès des Franciliens, **le Ceser invite la Région à utiliser tous ses canaux de communication afin de diffuser au plus grand nombre les *« bonnes pratiques d'hygiène numérique »*** recommandées par l'ANSSI et CyberMalveillance.

S'agissant plus spécifiquement des entreprises, l'attribution d'aides régionales, les actions de *networking* organisées avec le Réseau Île-de-France Entreprises et le Club ETI Île-de-France, par exemple, constituent autant d'occasions de diffuser au plus près les guides pratiques, publications ou offres de formation en ligne adaptées aux chefs d'entreprise.

Article 4 : Renforcer la formation des Franciliens aux enjeux de la citoyenneté numérique

Pour le Ceser, l'augmentation du risque numérique invite à **renforcer la formation de nos concitoyens aux enjeux de la sécurité et de la protection de la vie privée numérique, en portant une attention particulière aux jeunesses franciliennes,** qui exerceront demain des activités professionnelles ou bénévoles au sein des entreprises, collectivités et associations du territoire.

La Région, qui entretient des liens privilégiés avec les académies, les lycées et les universités franciliennes, pourrait ainsi :

- **Initier des campagnes de communication ciblées sur ces publics, dans le cadre de la mise en œuvre de la politique de sécurité du système d'information commune** aux trois académies franciliennes et à la Région ;
- **Faciliter l'intervention de médiateurs en cybersécurité** dans les établissements scolaires et universitaires, dans le prolongement des campagnes de lutte contre le (cyber)harcèlement qu'elle encourage et finance déjà ;
- **Embarquer des vidéos courtes de sensibilisation sur les ordinateurs portables** dont la Région équipe les élèves des lycées publics ;
- **S'assurer de la diffusion des ressources** créées pour ce public (par exemple celles proposées par CyberMalveillance) **via l'environnement numérique de travail MonLycée.Net** ;
- Envisager une action globale auprès du plus grand nombre de jeunes, scolarisés ou non, **en mobilisant les instituts de formation sanitaire et sociale, les résidences universitaires, les missions locales et espaces d'insertion** auxquels elle participe au financement.

[15] *CharteCyber* proposée par CyberMalveillance et signée par la Région Île-de-France à l'occasion du Mois européen de la cybersécurité.

Titre III – Répondre aux enjeux de structuration de la filière professionnelle de la cybersécurité en Île-de-France

Article 5 : Soutenir l'attractivité des formations de cette filière « en tension »

L'Île-de-France, qui réunit de nombreux centres de formation, entreprises du numérique et pôles d'excellence pour l'enseignement et la recherche, est la première région française pour la filière de la cybersécurité : elle concentre 54 % des professionnels[16] et 21 % des offres de formation[17] de la sécurité numérique. Pourtant, la filière reste considérée « en tension » au regard des besoins en compétences et en formation des entreprises – qui vont encore s'accroître avec le déploiement de la 5G, l'essor de l'internet des objets et de l'intelligence artificielle.

Aussi le Ceser recommande-t-il à la Région, compétente pour la formation et l'insertion professionnelle des jeunes et des demandeurs d'emploi :

- **De soutenir, notamment dans le cadre de l'agence Oriane, l'attractivité des métiers et des formations de la filière ainsi que leurs débouchés,** au regard des enjeux lourds de la cybersécurité pour la souveraineté économique régionale ;
- **D'inscrire dans la durée l'initiative du Campus des métiers et des qualifications « Métiers de la sécurité »,** en développant son offre de formation et de qualification dans le champ de la cybersécurité ;
- **De promouvoir le service public en ligne pour évaluer, développer, et certifier ses compétences numériques dénommé « Pix »** dans les formations proposées par l'agence Oriane.

Titre IV – Faciliter la coordination entre les acteurs de la prévention et de l'intervention sur le territoire régional

Article 6 : Accompagner la territorialisation des solutions de cyberprévention

Développer « le réflexe cyber » repose sur la mobilisation de toutes les parties-prenantes et appelle un effort de coordination pour accompagner la territorialisation des solutions de cyberprévention proposées aux entreprises, aux associations et aux collectivités franciliennes.

Pour le Ceser, la Région, si elle n'a bien sûr pas vocation à traiter seule le sujet, est légitime à **agir comme l'espace d'articulation entre les acteurs de la prévention et de l'intervention sur le territoire régional,** pour donner corps à l'ambition inscrite dans son SRDEII 2022-2028 : *« L'Île-de-France : un acteur régional de référence en Europe en matière de cybersécurité »*[18].

Le format des « Assises de la cybersécurité », organisées en 2018 par la Région, pourrait ainsi devenir **un rendez-vous annuel, dans le cadre du Mois européen de la cybersécurité,** pour entretenir la vigilance des acteurs, faire connaître de nouvelles solutions concrètes adaptées aux évolutions du risque numérique et attirer des jeunes talents, en articulant :

- La démonstration des solutions proposées par des prestataires régionaux pour valoriser l'écosystème régional ;
- La mise en relation directe (recherche de formation, de client ou de prestataire) ;
- L'organisation de simulations de cyberattaque et d'un « hackathon » pour faire émerger de nouvelles solutions, notamment pour les acteurs qui ne bénéficient pas des mesures déjà proposées par l'État ou la Région.

[16] *Les profils de la cybersécurité – Enquête 2021*, Observatoire des métiers de la cybersécurité, septembre 2021.
[17] *Observatoire GEN_SCAN - Rentrée 2023 : tendances de l'emploi et de la formation au numérique en France,* 2ème édition, Grande École du Numérique, octobre 2023.
[18] SRDEII 2022-2028, axe 1, sous-axe 1.2 : *« Protéger les TPE, PME et ETI contre l'exposition au risque grandissant de cyber-attaque »,* délibération du Conseil régional n° CR 2022-029, op. cit.

Article 7 : Aider à la création de postes de RSSI mutualisés

Le Ceser invite la Région Île-de-France, dans le cadre du développement progressif de son action en matière de sécurité numérique du territoire, à **s'engager dans le soutien (financement, équipement, fonctionnement, etc.) à la création de postes de Responsable de la sécurité des systèmes d'information (RSSI) mutualisés** entre petites collectivités, TPE et PME, et petites associations du territoire.

L'échelon départemental, voire intercommunal, apparaît pertinent pour développer ce maillage local d'acteurs agissant en complémentarité et en relais de l'EDIH (pôle européen régional d'innovation numérique) et du CSIRT régional, au bénéfice des structures ne disposant pas des moyens d'internaliser seuls cette compétence.

La mise en place d'un *« réseau régional de développeurs économiques visant notamment à renforcer le dialogue EPCI/Région »,* tel qu'annoncé dans la délibération du Conseil régional sur les orientations budgétaires pour 2024[19], peut constituer une occasion d'ouvrir une discussion sur le sujet avec les EPCI en partenariat avec les chambres consulaires, les fédérations professionnelles et les têtes de réseaux associatifs.

Article 8 : Orienter vers le programme Cybiah les PME qui en ont le plus besoin

La Région Île-de-France investit deux millions d'euros au titre du Fonds européen de développement régional (FEDER) dans le consortium Cybiah. Accueilli au Campus Cyber de La Défense et inscrit dans le réseau des pôles européens régionaux d'innovation numérique (*European Digital Innovation Hub* - EDIH), Cybiah développe un programme d'accompagnement à la maturité cyber des PME régionales, de la phase d'évaluation à l'implémentation d'une solution de cybersécurité adaptée. Cybiah participe également, en relation avec les seize EDIH régionaux du territoire national, à définir un référentiel commun aux prestataires de services de sécurité numérique, afin d'adresser une offre plus lisible et plus claire aux entreprises.

Le Ceser propose à la Région Île-de-France, en plus du soutien financier qu'elle accorde au consortium, **d'orienter vers Cybiah les PME du territoire qui ont le plus besoin de soutien**. Cette mise en relation constituerait une façon de prolonger l'investissement de la Région, particulièrement renforcé depuis la crise du Covid-19, pour soutenir toutes les entreprises du territoire en les aidant à prévenir de nouvelles difficultés nées du risque numérique.

Cet avis a été adopté :
Suffrages exprimés : 142
Pour : 141
Contre : 0
Abstentions : 1
Ne prend pas part au vote : 0

[19] Délibération n° CR 2023-052 : *Orientations budgétaires pour 2024,* adoptée par le Conseil régional le 16 novembre 2023.

CESER

Région îledeFrance

rapport

Cyberprévention : un enjeu de sécurité et de citoyenneté pour tous en Île-de-France

12 déc. 2023

Rapport présenté au nom de la commission
Développement économique
par **Bernard COHEN-HADAD** et **Vincent GAUTHERON**

Cyberprévention : un enjeu de sécurité et de citoyenneté pour tous en Île-de-France

Rapport présenté au nom de la commission Développement économique
par **Bernard COHEN-HADAD** et **Vincent GAUTHERON**

12 décembre 2023

CONSEIL ÉCONOMIQUE, SOCIAL ET ENVIRONNEMENTAL REGIONAL D'ÎLE-DE-FRANCE
2 rue Simone Veil • 93400 Saint-Ouen • Tél : 01 53 85 66 25 • Email : ceser@iledefrance.fr • www.ceser-iledefrance.fr

Abstract

Le risque numérique n'est pas une fatalité : s'il n'épargne plus personne (États, administrations, collectivités, établissements publics, entreprises, associations, personnalités et citoyens), des solutions existent pour s'en protéger.

Pourtant, on constate peu d'engagement opérationnel des entreprises, notamment les TPE-PME, comme des associations et des petites collectivités territoriales : la cyberprévention, condition essentielle de la cybersécurité et de la résilience du territoire francilien – dont l'exposition aux cyberattaques est particulièrement élevée – présuppose la prise de conscience de la réalité du risque numérique. Or, les enquêtes s'accordent sur le fait que cette prise de conscience est encore insuffisante.

Par ses compétences et le rôle qu'elle joue sur le territoire, en particulier pour les entreprises dont elle est une interlocutrice privilégiée, **la Région Île-de-France est légitime à agir.** Engagée dans un processus interne de transformation numérique, elle a par ailleurs fait de la *« défense de la souveraineté industrielle et numérique »* l'un des axes stratégiques de son Schéma régional de développement économique, d'innovation et d'internationalisation 2022-2028, dont les premières réalisations dans le champ de la cybersécurité se sont engagées à la rentrée 2023.

Ces initiatives sont récentes et il est bien trop tôt pour en évaluer la pertinence et l'efficience. Ce rapport et l'avis du Ceser Île-de-France se veulent **une contribution positive et attentive à une nouvelle politique publique régionale,** qui trouvera sa pleine maturité en s'inscrivant dans la durée et en s'adaptant à la diversité des acteurs concernés sur le territoire francilien.

L'enjeu est de « changer d'échelle » en accompagnant la structuration, l'adaptation (aux plus fragiles en particulier) et la territorialisation des solutions de cyberprévention, tout en développant l'information et la formation qui permettent à chacun de réduire son exposition au risque numérique.

Cet objectif appelle **un effort de coordination** pour assurer « le dernier kilomètre » de service auprès des entreprises, des associations et des collectivités franciliennes. Développer « le réflexe cyber » repose en effet sur la mobilisation de toutes les parties-prenantes : **la cyberprévention est une responsabilité collective, condition pour transformer les risques et défis en atouts ; elle constitue en cela un enjeu de sécurité et de citoyenneté.**

Sommaire

Introduction **3**
1 Le risque numérique n'épargne plus personne **4**
1.1 La cyberprévention, condition essentielle de la cybersécurité 4
1.2 Dans un contexte international troublé, le gain financier, l'espionnage et la déstabilisation constituent les principaux objectifs des cybercriminels 5
1.3 Les techniques exploitées par les cybercriminels se perfectionnent 6
1.4 Moins protégées et pour certaines inconscientes du risque numérique, TPME et ETI constituent de nouvelles cibles privilégiées pour les cybercriminels 9
1.5 L'insécurité numérique est synonyme d'insécurité économique 11
1.6 L'assurance contre le risque cyber : une solution sous conditions 14
2 Au croisement d'enjeux multiples, la cybersécurité est une responsabilité collective **17**
2.1 Un enjeu de conformité à une réglementation mouvante et complexe 17
2.2 Un enjeu d'adaptation aux nouvelles pratiques du travail et de la consommation 18
2.3 Un enjeu de lisibilité et d'accessibilité de l'offre de services aux entreprises 19
2.4 Un enjeu de structuration de la filière professionnelle 22
2.5 Un enjeu de culture d'entreprise 24
2.6 Un enjeu éducatif 27
3 Panorama des solutions proposées aux acteurs économiques franciliens **28**
3.1 La cybersécurité s'inscrit dans une stratégie européenne et nationale 28
3.1.1 L'Agence nationale de la sécurité des systèmes d'information, autorité de référence au plan national pour les opérateurs vitaux 28
3.1.2 Cybermalveillance : le service public d'information, de prévention et de réaction aux cyberattaques pour le grand public 30
3.1.3 L'Observatoire de la sécurité des moyens de paiement 31
3.1.4 Cyberscore et filtre anti-hameçonnage « grand public » : deux nouveaux dispositifs nationaux en cours de déploiement 32
3.2 Les acteurs-clés de la prévention et de la gestion des incidents de sécurité numérique en Île-de-France 34
3.2.1 Le consortium régional Cybiah au sein du Campus Cyber de La Défense 34
3.2.2 L'accompagnement financier des acteurs économiques par la Région 35
3.2.3 UrgenceCyber Île-de-France, la « cybercaserne » régionale 39
3.3 La coordination des acteurs est essentielle pour assurer la meilleure protection au territoire francilien 41
Conclusion **42**
Remerciements **43**
Liste des membres de la commission Développement économique **44**
Glossaire **45**
Bibliographie **46**
Annexes **51**
CharteCyber proposée par CyberMalveillance et signée par la Région Île-de-France 51
Présentation du nouveau dispositif « Chèque Cyber » de la Région Île-de-France 52

Introduction

La transformation numérique, nourrie par l'augmentation rapide du taux d'équipement des particuliers et des professionnels en terminaux et objets connectés, permet la dématérialisation croissante de démarches et services – dans le secteur public comme dans le privé – et fait **basculer les entreprises, associations et collectivités de toutes tailles dans une économie de la donnée.** Désormais essentielle pour la gestion quotidienne de ces organismes, la donnée représente également un gisement de valeur pour les citoyens, dans leur vie personnelle et professionnelle.

Si cette valeur peut être positivement exploitée, par exemple pour renforcer l'information des citoyens, proposer de nouveaux produits, des services innovants, etc., **elle est aussi une source d'intérêt pour une nouvelle criminalité :** les failles technologiques des équipements et logiciels, la méconnaissance ou le manque de vigilance de leurs utilisateurs, constituent autant de sources potentielles de profit pour ceux qu'il est convenu de qualifier de « cybercriminels ».

Les entreprises sont les premières concernées par leurs attaques : selon l'Agence nationale de sécurité des systèmes d'information (ANSSI), qui fait autorité en la matière au plan national, 40 % des attaques au rançongiciel déclarées en 2022 ont visé des entreprises, qu'elles soient très petites (TPE), moyennes (PME) ou de taille intermédiaire (ETI). Les attaques ont tendance à se déporter vers ces acteurs, qui sont à la fois structurellement plus vulnérables et moins bien protégés que les grands organismes publics et les grandes entreprises. Une cyberattaque peut être fatale : plus d'une TPME sur deux et, selon les sources, jusqu'à trois sur quatre, déposerait le bilan dans les trois ans qui suivent une cyberattaque réussie. **Enjeu politique, la cybermenace est donc aussi un enjeu économique.**

Les pouvoirs publics se mobilisent et multiplient les initiatives pour développer l'information et la sensibilisation des acteurs. Ils investissent dans des solutions pour accompagner le traitement de ces attaques et en limiter les effets. **Par ses compétences et le rôle qu'elle joue sur le territoire, en particulier pour les entreprises, la Région Île-de-France est légitime à agir :** elle a en effet fait de la « défense de la souveraineté industrielle et numérique » l'un des axes stratégiques de son Schéma régional de développement économique, d'innovation et d'internationalisation (SRDEII) 2022-2028[1].

À l'occasion de la première édition du « Forum de la sécurité économique et numérique » à destination des TPE-PME et des collectivités, organisé par le ministère chargé de l'Économie, l'ANSSI, la préfecture de région, la Région Île-de-France et la Chambre de commerce et d'industrie (CCI) Paris Île-de-France fin 2022, **le Conseil régional a annoncé le lancement de son propre plan d'actions dont les premières applications concrètes sont engagées en 2023.**

Sensible aux enjeux de transformation et d'adaptation des entreprises, ainsi qu'aux solutions opérationnelles proposées pour y répondre, **le Ceser a choisi de se saisir du sujet en portant une attention particulière à la prévention du risque cyber pour les acteurs économiques et leurs collaborateurs,** compte tenu de leur fort niveau d'exposition, à partir d'une analyse de leurs enjeux.

Les initiatives publiques et privées, notamment celles étudiées dans le cadre de ce rapport, sont récentes : il est bien trop tôt pour en évaluer la pertinence et l'efficience. Ce rapport – tout comme les recommandations de l'avis qu'il introduit – doit être compris comme **une contribution au débat et à l'effort de mobilisation collective.**

[1] Délibération du Conseil régional n° CR 2022-029, adoptée le 19 mai 2022.

1 Le risque numérique n'épargne plus personne

1.1 La cyberprévention, condition essentielle de la cybersécurité

La cybersécurité s'entend comme *« l'état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace »*[2], constitué par les infrastructures interconnectées relevant des technologies de l'information et par les données qui y sont traitées.

Elle est assurée par la cyberprotection[3] ainsi que, dans le cas des États et organismes jugés d'importance vitale, par la cyberdéfense[4], qui reposent sur l'analyse tant des faiblesses technologiques des systèmes d'information que des vulnérabilités liées à leurs usages, afin de mettre en place des outils et des stratégies pour en réduire la surface d'exposition aux cyberattaques[5]. Ces démarches sont appelées à évoluer en permanence, en fonction des menaces qui peuvent être détectées ou subies, des normes de sécurité définies par les autorités compétentes et de l'évolution des protocoles informatiques.

Le droit[6] ne définit pas les termes de « cyberdélinquance » ou de « cybercriminalité » mais définit un ensemble d'infractions et de peines échelonnées pour les délits et crimes commis *via* ou à l'encontre du bon fonctionnement ou de l'intégrité d'un système d'information. Ceux-ci peuvent donc être à la fois des nouveaux supports d'infractions antérieures à l'ère numérique (escroquerie, chantage, etc.) mais aussi des cibles en tant que telles (diffusion de virus informatique, pénétration non autorisée dans tout ou partie d'un système d'information pour en perturber le bon fonctionnement, etc.). Le terme « cybercriminalité[7] » tend à s'imposer dans le débat public, sans doute par traduction littérale du terme anglo-saxon *cybercrime*, qui qualifie tous les types d'infractions sans distinction.

Sur le plan pénal, les cyberattaques caractérisées s'organisent en trois catégories principales[8] :
- escroquerie (attaques sur les virements, *phishing*, piratage de données, etc.) : 77 %,
- atteinte aux personnes (diffamation, harcèlement, incitation à la haine, etc.) : 13 %,
- atteintes aux traitements et systèmes automatisés de données : 10 %.

La cybercriminalité accompagne la croissance des usages de l'internet. Rappelons que **plus de neuf Français sur dix sont aujourd'hui connectés[9],** à la faveur d'un taux d'équipement en croissance, notamment en smartphones (87 % des 12 ans et plus, + 3 points par rapport à 2020) et en objets connectés (40 % des 12 ans et plus, + 7 points par rapport à 2020). Raison pour laquelle l'Organisation de coopération et de développement économiques (OCDE) substitue au terme de cybersécurité celui de « sécurité numérique », en réponse au **besoin fort de sécurisation des**

[2] Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire de la défense, JORF du 19 septembre 2017, consulté sur le portail FranceTerme administré par le ministère de la Culture.
[3] *« Ensemble des moyens, techniques ou juridiques, qui contribuent à assurer la cybersécurité ; la cyberprotection s'appuie, notamment, sur des mesures prises pour préserver la sécurité des systèmes d'information. »* Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire de la défense, op. cit.
[4] « *Ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité. »* Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire de la défense, op. cit.
[5] *« Ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité. Une cyberattaque peut être ponctuelle, ou s'inscrire dans la durée en mobilisant des moyens humains et techniques importants pour infiltrer durablement les systèmes d'information vitaux d'une organisation : on parle alors de « cyberattaque persistante ».* Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire de la défense, op. cit.
[6] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite « loi Godfrain », JORF du 6 janvier 1988 : ses dispositions initiales ont été codifiées et modifiées par plusieurs lois successives, dans le code pénal, Livre III : *Des crimes et délits contre les biens*, Titre II : *Des autres atteintes aux biens*, Chapitre III : *Des atteintes aux systèmes de traitement automatisé de données* (articles 323-1 à 323-8).
[7] *« Ensemble des infractions pénales qui sont commises dans le cyberespace ».* Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire du droit, JORF du 7 décembre 2018, consulté sur le portail FranceTerme administré par le ministère de la Culture.
[8] D'après le préfet de BOUSQUET, *senior advisor* au sein du groupe Adit, entendu en audition par la commission Développement économique du Ceser Île-de-France le 1er juin 2023.
[9] D'après le *Baromètre du numérique 2022*, publié par le ministère délégué chargé de la Transition numérique et des télécommunications avec l'ARCEP, l'ARCOM, l'ANCT et le Conseil général de l'économie, 30 janvier 2023.

outils et systèmes de traitement automatisé de données qui agissent sur notre quotidien, dans un contexte de transformation numérique qui s'accélère.

La cyberprévention, objet de ce rapport, présuppose la prise de conscience de ce « risque numérique[10] » et donc la connaissance des mécanismes des cyberattaques comme des moyens de s'en prémunir. Elle est une condition essentielle de la cybersécurité et de la cyberrésilience, entendue comme *« la capacité d'un système d'information à résister aux cyberattaques et aux pannes accidentelles, puis à revenir à un état de fonctionnement et de sécurité satisfaisant »*[11].

1.2 Dans un contexte international troublé, le gain financier, l'espionnage et la déstabilisation constituent les principaux objectifs des cybercriminels

Nées avec l'essor de l'internet, **les cyberattaques connaissent une croissance continue,** nourrie à la fois d'une appropriation croissante des techniques d'agression par les réseaux criminels et d'une industrialisation de ces processus d'agression[12]. Les intrusions avérées dans des systèmes d'information signalées à l'Agence nationale de la sécurité des systèmes d'information (ANSSI, voir aussi p. 28) ont bondi de 37 % entre 2020 et 2021, pour atteindre jusqu'à trois par jour[13]. Un quart des incidents traités ont lieu en Île-de-France.

Dans son *Panorama annuel de la cybermenace*, l'ANSSI fait état des grandes tendances du risque numérique et de ses évolutions. La dernière édition 2022 révèle **un niveau général de menace élevé, dans un contexte géopolitique sensible** qui renforce les menaces de déstabilisation contre les systèmes d'informations de l'État et des opérateurs d'importance vitale[14] (OIV).

Les principales motivations des cybercriminels (ou de leurs donneurs d'ordre), outre la prédation financière, relèvent du sabotage (pour faire tomber un concurrent), de l'espionnage industriel (vol de brevets ou de données techniques) ou commercial (vol de données clients), ou de la tentative de déstabilisation, voire d'entrave (ciblant plus particulièrement les administrations et l'État)[15].

Si les attaques perpétrées contre des établissements publics font régulièrement la une de la presse, la menace d'espionnage informatique, plus discrète et silencieuse, demeure importante et permanente : leur détection et leur traitement représentent plus de 80 % des activités de l'ANSSI qui a compétence directe en la matière. Les méthodes de ce « cyberespionnage[16] » sont marquées par des évolutions technologiques très rapides et une montée en compétence permanente des attaquants. Les entreprises qui agissent à l'export sont appelées à une attention particulière (notamment lors du déplacement de leurs collaborateurs à l'étranger) par le Service de l'information stratégique et de la sécurité économiques (Sisse) rattaché à la direction générale des entreprises.

Le conflit russo-ukrainien offre un contexte favorable à l'augmentation des actions de déstabilisation. Si les attaques par sabotage ont été jusqu'à présent relativement limitées aux systèmes ukrainiens, l'évolution du conflit et l'engagement des États européens aux côtés de l'Ukraine peut constituer une motivation supplémentaire de lancement d'attaques ciblées.

Plus largement, le contexte de guerre économique entre États, notamment dans le secteur de l'énergie, encourage certains à recourir à des acteurs offensifs privés pour dissimuler le donneur d'ordre.

---

[10] De la même manière, Campus Cyber parle de « risque numérique » plutôt que de « risque cyber ». Audition d'Anne-Sophie COLLÉAUX, coordinatrice de l'EDIH Cybiah, par la commission Développement économique du Ceser Île-de-France, le 30 juin 2023.
[11] Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire de la défense, op. cit.
[12] Audition du préfet de BOUSQUET, 1er juin 2023.
[13] *Panorama de la menace informatique 2021*, Agence nationale de la sécurité des systèmes d'information, 9 mars 2022.
[14] *« Personne morale publique ou privée qui gère ou utilise des établissements ou des ouvrages dont la destruction ou même l'indisponibilité obéreraient gravement le potentiel militaire, la force économique, la sécurité, voire la capacité de survie d'un État, ou mettraient en danger sa population ».* Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire de la défense, op. cit. La liste de ces OIV n'est pas publique pour des raisons de sécurité.
[15] Audition du préfet de BOUSQUET, 1er juin 2023.
[16] *« Ensemble d'actions menées dans le cyberespace consistant à infiltrer, clandestinement ou sous de faux prétextes, les systèmes informatiques d'une organisation ou d'un individu, et à s'emparer de données pour les exploiter ».* Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire du droit, JORF du 31 août 2019, consulté sur le portail FranceTerme administré par le ministère de la Culture.

Enfin, **l'accueil sur le territoire français de grands évènements internationaux** (Coupe du monde de rugby 2023 puis l'édition 2024 des Jeux olympiques et paralympiques) **renforce l'exposition aux attaques des systèmes d'informations des opérateurs et acteurs économiques nationaux et régionaux** – l'Île-de-France étant territoire hôte de ces deux compétitions. À titre d'illustration : la société Atos, supporter officiel en services et opérations de cybersécurité pour le Comité d'organisation des Jeux (COJO), s'attend à entre huit et dix fois plus d'attaques qu'à Tokyo où 4,5 milliards d'attaques avaient été repoussées[17].

1.3 Les techniques exploitées par les cybercriminels se perfectionnent

Les cyberattaques exploitent prioritairement trois failles :

- les usages numériques insuffisamment ou non maîtrisés,
- les faiblesses dans la sécurisation des données, notamment dans le travail en réseau (recours à l'informatique en nuage ou cloud, externalisation de services et données auprès d'entreprises de services numériques, réseaux wifi publics ouverts, etc.),
- les défauts de construction ou de programmation d'un logiciel ou d'un système d'exploitation, qui ouvrent des failles de vulnérabilité tant qu'ils ne sont pas corrigés : ces failles peuvent d'ailleurs faire l'objet d'un commerce entre hackeurs et réseaux criminels – voire entre hackeurs et fabricants/concepteurs, qui peuvent être prêts à payer des sommes conséquentes pour identifier ces failles et les corriger (notamment pour des failles dites *« zero-day »* pour lequel aucun correctif n'a encore été publié).

Les cyberattaques peuvent être ciblées, mais aussi générales : en permanence, des robots informatiques « scannent » le matériel informatique ou les systèmes d'information, cherchent la faille, souvent à l'insu de leur propriétaire. Ainsi la pénétration réussie d'un système d'information n'entraîne pas forcément le déclenchement d'une attaque immédiate, qui peut se produire plusieurs semaines, voire plusieurs mois après si la vulnérabilité n'a pas été détectée et corrigée.

Les investigations des services de sécurité informatique révèlent une grande créativité des cybercriminels. Elles constatent à la fois une grande diversité des souches de logiciel malveillant (*malware*), code informatique conçus pour infecter, endommager ou accéder à des systèmes informatiques ; et une extension du phénomène, autrefois concentré dans certaines régions du monde (il y a vingt ans, la Corée du Nord était pionnière dans l'extorsion de devises par cyberattaque). On assiste également à **l'essor de réseaux spécialisés dans la conception, la mise en œuvre et le déploiement de cyberattaques** qui « revendent » leurs solutions à d'autres réseaux criminels (*crime-as-a-service*).

L'hameçonnage[18] *(phishing)* constitue le premier levier des cybercriminels pour pénétrer un système d'information protégé en exploitant la méconnaissance ou la faute des utilisateurs : fausse annonce, faux documents, lien vers un site internet « officiel » contrefait, envoyés en masse pour toucher un maximum de cibles potentielles.

Les rançongiciels *(ransomware)* sont le levier d'attaques plus sophistiquées qui suppriment l'accès de l'entreprise ou de la collectivité à ses données, et/ou génèrent un vol de données, assortis **d'une tentative d'extorsion de fonds par chantage** : l'entreprise est invitée à payer une rançon dans un délai très court – parfois en cryptomonnaie et sur un compte bancaire localisé dans un pays sans accord de collaboration judiciaire avec la France – sous réserve de perdre définitivement ses données ou qu'elles soient revendues à la concurrence ou à des réseaux criminels spécialisés. Les *hackers* révèlent en général une fraction des données volées, à la fois pour crédibiliser la demande de rançon et apeurer leurs futures victimes. L'attaque par rançongiciel est prisée par les réseaux criminels puisqu'elle représente une source rapide de gains importants.

[17] D'après Bernard GIRY, directeur du pôle Transformation numérique de la Région Île-de-France, entendu en audition par la commission Développement économique du Ceser Île-de-France le 5 septembre 2023.

[18] *« Technique de fraude visant à obtenir des informations confidentielles, telles que des mots de passe ou des numéros de cartes de crédit, au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales ».* Source : Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire du droit, JORF du 14 septembre 2021, consulté sur le portail FranceTerme administré par le ministère de la Culture.

Selon Hiscox, 63 % des victimes de rançongiciel paieraient la somme exigée[19], pour régler le problème rapidement, pour récupérer leurs données ou pour cacher la situation, par peur de perdre leur clientèle, voire leur affaire[20]. Le préjudice peut s'élever de quelques milliers d'euros pour des particuliers à plusieurs dizaines ou centaines de milliers voire millions d'euros pour les plus grandes structures : ainsi, en août 2021, le centre hospitalier sud-francilien de Corbeil-Essonnes s'est vu réclamer une rançon de 10 millions de dollars par un groupe de hackers russes. Le règlement de la rançon ne garantit nullement la restitution des données dans leur intégralité (seules 32 % des entreprises attaquées déclarent avoir récupéré une partie de leur données), ni n'empêche leur revente (25 % de ces entreprises déclarent que leurs données ont « fuité » malgré le paiement de la rançon exigée). Elle ne permet pas non plus de garantir la restauration de l'intégrité du système d'information (33 % de ces entreprises ont dû le reconstruire malgré le téléchargement de la clef de déchiffrement fournie après paiement de la rançon) ni l'absence de réitération de l'attaque (par exemple si le téléchargement de cette clef s'accompagne de l'installation d'un logiciel de prise de contrôle à distance d'un poste : 20 % de ces entreprises déclarent avoir subi une seconde attaque). Elle peut par ailleurs entrainer un risque de poursuite administrative ou judiciaire pour complicité de financement du terrorisme ou blanchiment d'argent lorsque l'attaque est commanditée par des organisations terroristes ou des personnes figurant sur des listes de sanctions internationales.

Parmi les autres modes d'attaque repérés, les cybercriminels peuvent aussi recourir à l'attaque par force brute *(bruteforce attack)* qui consiste à tester, l'une après l'autre, chaque combinaison possible d'une clé de cryptage pour un identifiant donné afin se connecter au système visé. L'objectif peut être **le vol de données, la saturation ou l'effondrement d'un système d'information.**

À côté de ces modes d'attaque qui reposent prioritairement sur l'exploitation de failles technologiques, **se développent des techniques de fraude « par ingénierie sociale »** basées sur la collecte de données sur les dirigeants d'entreprise (pour crédibiliser la fraude), l'usurpation d'identité et la pression sur les collaborateurs (pour manipuler les salariés dans le sens de l'intention des criminels). Parmi celles-ci :

- **L'usurpation d'identité du ou des dirigeants de l'entreprise ou de l'organisme ciblé** (technique du *big-game hunting*) pour forcer un virement « urgent » vers un compte bancaire inconnu du service en charge de réaliser les paiements – d'après la Banque de France[21], la technique de la « fraude au président », qui s'était déplacée des grandes entreprises vers les TPME, semble connaître un regain d'activité en 2022, notamment sur les PME/ETI ;
- **La fraude au « faux conseiller bancaire », ou l'usurpation d'identité d'un fournisseur ou d'un créancier** avec lequel une entreprise ou un organisme est réellement en relation, pour substituer à leurs coordonnées bancaires authentiques celles des fraudeurs ;
- **L'arnaque au faux support technique,** permettant à un « faux technicien » d'obtenir l'autorisation d'accès (physique ou informatique) au système d'information de l'entreprise ou de l'organisme ciblé, sous le prétexte de corriger une faille de sécurité.

[19] Source : *Rapport Hiscox 2023 sur la gestion des cyber-risques*, 7ème édition, publié le 10 octobre 2023. Le rapport repose sur une enquête en ligne internationale (États-Unis, Royaume-Uni, France, Allemagne, Espagne Belgique, République d'Irlande et Pays-Bas) menée par Forrester Consulting auprès de plus de 5 000 professionnels en charge de la stratégie de cybersécurité de leur entreprise (dont plus de 900 pour la France seule).
[20] Audition du préfet de BOUSQUET, 1er juin 2023.
[21] Audition de Julien LASALLE, adjoint au directeur des études et de la surveillance des paiements de la Banque de France, par la commission Développement économique du Ceser Île-de-France, 1er juin 2023.

Focus : La fraude aux moyens de paiement

Les transactions financières entre les entreprises et leurs fournisseurs, leurs prestataires, leurs clients et consommateurs représentent aussi une source potentielle d'insécurité.

En application de l'art. L141-4 du code monétaire et financier, la Banque de France veille au bon fonctionnement et à la sécurité des systèmes et moyens de paiement scripturaux[22] ainsi qu'à la pertinence des normes applicables en la matière. Cette mission l'amène à contrôler l'action des banques, en sus de l'Autorité de contrôle prudentiel et de résolution (ACPR), des réseaux de paiement par carte bancaire et des différents prestataires opérant dans le traitement des flux de paiement, y compris la gestion des solutions de paiement des commerçants.

Selon les données de la Banque de France, les paiements scripturaux ont représenté en 2021 42 200 milliards d'euros (soit plusieurs fois le montant annuel du produit intérieur brut) dont 92 % de virements, majoritairement entre professionnels ; et 28 milliards de transactions, dominées par les consommateurs pour des petits paiements effectués à 59 % par carte bancaire.

Parmi les modes de paiement scripturaux utilisés, les services de la Banque de France enregistrent un développement important du paiement « sans contact » (+ 31 % au 1er semestre 2022 par rapport à l'année 2021), incluant le paiement via mobile ou appareil connecté (+ 131 %). A l'inverse, le chèque, moyen de paiement le plus utilisé en France jusqu'aux début des années 2000, poursuit sa perte de vitesse (bien que la France reste le second pays au monde en termes d'émission de chèques rapportée au nombre d'habitants, après les États-Unis).

En quoi consiste la fraude aux moyens de paiement ?

La fraude aux moyens de paiement est définie comme l'utilisation illégitime d'un moyen de paiement ou des données qui lui sont attachées, ayant pour conséquence un préjudice financier constaté (le fait de collecter de l'information dans gain financier n'est pas caractérisé comme de la fraude), quels que soit le mode opératoire et l'identité du fraudeur (qui peut d'ailleurs être l'utilisateur du moyen de paiement lui-même). La fraude se distingue de la « tentative de fraude » : tout comme dans le milieu de la cybercriminalité, on constate une spécialisation de réseaux criminels dans la captation de données bancaires qu'ils revendent à d'autres réseaux qui les utiliseront à leur tour pour commettre une infraction caractérisée comme une fraude.

Le montant total de la fraude aux moyens de paiement scripturaux en 2021 s'élève à 1,24 milliard d'euros (+ 8,5 %par rapport à 2020) opérés via 7,5 millions de transactions frauduleuses (- 3,8 %) :

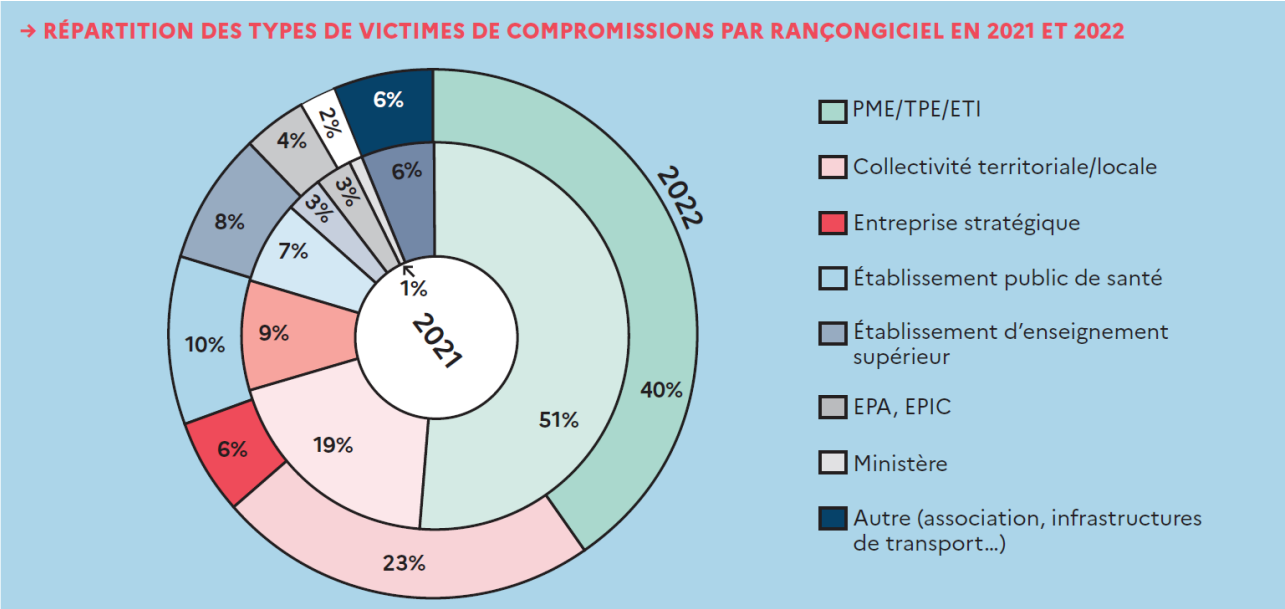
- **Le chèque constitue la principale source de fraude** avec 37 % des fraudes enregistrées ;
- **Le paiement par carte bancaire représente 34 % des sources de fraudes constatées,** essentiellement dominées par le paiement à distance. La fraude au moyen de paiement en point de vente est quasi nulle : d'une part, les montants sont plutôt faibles, donc peu intéressants pour des fraudeurs, d'autre part ce risque est généralement couvert par les établissements bancaires. Il faut distinguer les moyens de paiement « 100 % sans contact » et sans authentification, associés à un plafond paiement bloqué, des cartes ou terminaux mobiles équipés de dispositifs d'authentification (notamment biométriques), pour lesquels il n'y a pas de plafond ;
- L'analyse de **la fraude au virement, qui réunit 23 % des fraudes constatées,** est plus complexe car elle mêle virements entre professionnels et entre particuliers, qui n'opèrent pas des mêmes circuits ni ne représentent les mêmes montants fraudés. **Le virement télématique, utilisé exclusivement par les professionnels, ne représente que 7 % des fraudes mais pour un montant unitaire moyen de 80 000 euros environ,** ce qui peut dégrader très rapidement la trésorerie d'une entreprise.

Pour les moyens de paiement électroniques, les canaux d'utilisation à distance restent les principales cibles des fraudeurs. Mais les modes opératoires se déportent progressivement vers des techniques de manipulation relevant de la fraude à l'ingénierie sociale (cf. p. 7).

[22] Aux termes de l'art. L311-3 du code monétaire et financier : *« sont considérés comme moyens de paiement tous les instruments qui permettent à toute personne de transférer des fonds, quel que soit le support ou le procédé technique utilisé » ;* la définition exclue donc le paiement en espèces.

1.4 Moins protégées et pour certaines inconscientes du risque numérique, TPME et ETI constituent de nouvelles cibles privilégiées pour les cybercriminels

La menace cybercriminelle accuse une croissance continue et s'ajoute aux fragilités nées de la crise liée à la pandémie du Covid-19 et au contexte inflationniste. La cybercriminalité liée aux rançongiciels connaît même un regain d'activités en France fin 2022. Dans son *Panorama* 2022, l'ANSSI constate par ailleurs que ce type d'attaques a tendance, depuis quelques années, à *« se déporter des opérateurs régulés vers des entités moins bien protégées »* : les TPE, PME et ETI (40 % des rançongiciels traités ou rapportés à l'ANSSI en 2022, hors *« entreprises stratégiques »*), les collectivités territoriales (23 %) et les établissements publics de santé (10 %).



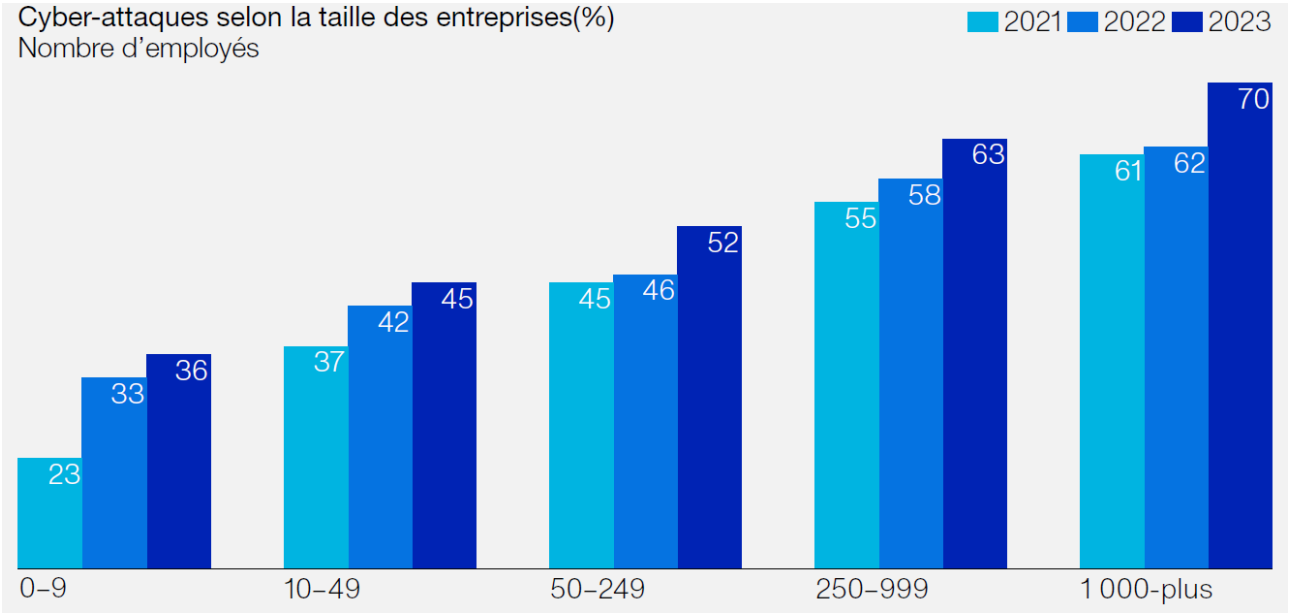
Source : *Panorama de la cybermenace 2022*, Agence nationale de la sécurité des systèmes d'information, 24 janvier 2023.

Ces données ne prennent en compte que les incidents signalés à l'ANSSI et méconnaissent le *« chiffre noir »* évoqué par l'ensemble des experts auditionnés par le Ceser, qu'il est difficile d'estimer même si les sources convergent pour en signaler l'augmentation continue : **la réalité des attaques contre des TPE, PME et ETI est donc sans doute encore plus importante.** Les cyberattaquants ont élargi leur cible première : même une TPE ne détenant pas de données particulièrement sensibles peut être la cible d'une cyberattaque ; ainsi, *« au cours des trois dernières années, le nombre d'entreprises de moins de dix salariés ayant subi une attaque* [dans le monde] *a augmenté de plus de moitié pour atteindre 36 % »,* selon le groupe d'assurance Hiscox.

Que faire en cas de cyberattaque avérée ?

En cas d'attaque avérée, l'ANSSI recommande :

- **De ne surtout pas payer la rançon exigée :** rien ne garantit que le paiement de la rançon ne permettre à l'entreprise visée de récupérer les données volées ou confisquées ;
- **De ne pas chercher à intervenir soi-même, sans appui technique certifié,** sur les systèmes d'information infectés : le risque étant d'aggraver la portée de l'attaque ;
- **De porter plainte** afin que l'attaque soit remontée aux services compétents, et que l'analyse de la cyberattaque permette de compléter les connaissances disponibles pour en prévenir d'autres ;
- **De s'adresser à un expert qualifié** pour les interventions d'urgence sur les systèmes attaquées et leur remise en service dans des conditions améliorées de sécurité informatique.



Source : *Rapport Hiscox 2023 sur la gestion des cyber-risques*, 10 octobre 2023, op. cit.

Pourtant, une grande majorité des TPME se dit convaincue par le numérique[23] : pour 76 % d'entre elles, le numérique représente *« un bénéfice réel »* ; pour 39 % d'entre elles, il est identifié comme une source supplémentaire de chiffre d'affaires. Une entreprise sur deux (51 %, en forte progression annuelle : + 8 points par rapport à l'année 2022) capte désormais au moins 5 % de ses clients en ligne. En conséquence, la présence des TPME sur internet se généralise : 84 % d'entre elles déclarent disposer d'au moins une solution de visibilité en ligne, 67 % ont un site internet et 35 % sont actives sur les réseaux sociaux. En moyenne, 27 % des TPME interrogées ont mis en place une solution de vente en ligne, avec de fortes variations selon les secteurs d'activité, hébergement/restauration (51 %) et commerce (47 %) en tête.

Dans cette progression choisie ou subie à mesure que la transformation numérique s'impose à toutes les entreprises, **on peut regretter que « seulement » 48 % des dirigeants de TPME interrogés expriment des craintes relatives à la sécurité des données de leur entreprise** – et se féliciter dans le même temps que cet indicateur progresse de 12 points par rapport à 2020[24]. C'est à la fois un signe encourageant de l'effet des messages de sensibilisation et des mesures prises par les acteurs économiques et les pouvoirs publics, et le **révélateur d'une prise de conscience du risque encore insuffisante**. Qui plus est, cette perception du risque est volatile et dépend fortement du contexte économique, qui influe sur la hiérarchie des risques (sociaux, matériels, concurrence, etc.) perçus par les dirigeants.

Si les TPME et les ETI constituent une cible privilégiée des cybercriminels, c'est parce qu'elles leur apparaissent plus vulnérables. Les experts entendus en audition par le Ceser pointent un certain nombre de *« failles structurelles[25] »* de ces catégories d'entreprises :

- **Un niveau de sécurité insuffisant :** seul un tiers des TPME déclare au moins un collaborateur « dédié à l'informatique » en charge de la cybersécurité dans leur entreprise[26], et le recours à des prestataires externes pour la gestion de données en cloud sans clause de cybersécurité suffisante accroît la surface de risque. Pour les autres, il s'agit soit du chef d'entreprise directement (41 %), soit une autre personne (8 %) ou encore pour près d'une TPME sur cinq, personne n'est spécifiquement dédié à la cybersécurité. La prise en compte de l'enjeu augmente toutefois avec la taille de l'entreprise ;

[23] *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023,* étude réalisée pour FranceNum par Centre de recherche pour l'étude et l'observation des conditions de vie (Crédoc), septembre 2023. FranceNum est une initiative gouvernementale pour la transformation numérique des TPE/PME pilotée par la Direction générale des entreprises (ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique) en partenariat, notamment, avec Régions de France.
[24] *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023,* FranceNum / Crédoc, op. cit.
[25] Audition d'Anne-Sophie COLLÉAUX, 30 juin 2023.
[26] *Les TPE/PME et la cybersécurité*, enquête Ipsos/XEFI, décembre 2021.

- **Des ressources limitées :** ressources financières pour s'équiper, ressources humaines pour internaliser la gestion du risque – or la ressource qualifiée est rare et donc chère, en particulier pour les petites structures ;
- **Le manque de prise de conscience ou de maîtrise du sujet par un grand nombre de dirigeants d'entreprises,** qui peuvent les conduire à créer des postes de directeur des systèmes d'information (DSI) ou de responsable de la sécurité des systèmes d'information (RSSI) gérés comme des emplois fonctionnels, moins valorisés qu'une fonction opérationnelle (moins « écoutés » par l'encadrement supérieur de l'entreprise, moins rémunérés donc moins attractifs) ;
- **Une méconnaissance des responsabilités de chacun** qui peut nourrir la tentation de reporter la charge de la gestion du risque sur les pouvoirs publics.

Ce manque de connaissance peut aussi pousser des dirigeants de PME et d'ETI à faire des choix de gestion susceptibles d'accroître leur exposition au risque numérique[27], en n'intégrant pas suffisamment la cybersécurité *by design* dans leurs projets de développement :

- développement « à marche forcée » d'activités (par ex : la réponse à un marché public), pression sur la réalisation ou la mise en production : or la sécurité informatique, qui doit conjointement évoluer avec l'activité, peut rallonger les délais et renchérir les coûts de développement d'un nouveau produit,
- développement de nouvelles fonctionnalités / solutions informatiques, sans mise en cohérence avec le système informatique « cœur » déjà en place.

Moins protégées et moins conscientes du risque numérique, **les TPME peuvent aussi être utilisées comme des « chevaux de Troie » pour atteindre des cibles mieux protégées dont elles font partie de la chaîne logistique** – à l'image, par exemple, de la cyberattaque dont a été victime l'établissement André-Mignot du centre hospitalier de Versailles à Le Chesnay-Rocquencourt (Yvelines) en décembre 2022, dont le système d'information a été pénétré via une petite entreprise prestataire. Ces attaques « en rebond » pénalisent directement l'activité des TPME concernées et sont également susceptibles d'engager leur responsabilité.

1.5 L'insécurité numérique est synonyme d'insécurité économique

Selon le Club des experts de la sécurité de l'information et du numérique (CESIN)[28], **60 % des responsables de la sécurité des systèmes d'information estiment que les cyberattaques dont ont été victimes leurs entreprises ont entrainé un impact direct sur leur activité :**

- perturbation de la production,
- perte de chiffre d'affaires à la suite de ventes non réalisées,
- atteinte à l'image auprès des investisseurs et des clients,
- risque légal et pénalités liées à une rupture contractuelle des engagements de la société,
- perte de propriété intellectuelle ou de données,
- perte financière directe liée à des transactions frauduleuses.

[27] Audition d'Anne-Sophie COLLÉAUX, 30 juin 2023.
[28] *Baromètre annuel de la cybersécurité des entreprises, 8ème édition*, réalisé par OpinionWay pour le Club des experts de la sécurité de l'information et du numérique (CESIN), 30 janvier 2023.

Source : *Cyberattaque : quel coût pour une TPE / PME ?,* Astrid Marie Pirson, Hiscox, 21 juillet 2020, in *La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?,* rapport d'information n° 678 (2020-2021) de MM. Sébastien MEURANT et Rémi CARDON, fait au nom de la délégation aux entreprises du Sénat, 10 juin 2021.

Le coût moyen d'une cyberattaque « réussie » est estimé en France en 2022 à 58 600 euros[29], une moyenne qui recouvre des réalités disparates selon le type et la portée de l'attaque tout comme la taille de l'organisation ciblée. Ce coût se décompose entre :

- un coût direct (25 600 euros, soit 44 % du montant global), qui prend en compte les ressources allouées à la résolution de la crise (mobilisation des équipes internes, recours à des services externes pour la restauration du système d'information, honoraires juridiques, frais de communication de crise, etc.),
- le coût de la rançon (25 700 euros, soit 44 %),
- et les coûts induits par l'interruption d'activité (7 300 euros, soit 12 %).

Une attaque informatique peut donc conduire une entreprise à disparaître, notamment les plus fragiles : **plus d'une TPME sur deux et, selon les sources, jusqu'à trois sur quatre, déposerait le bilan dans les trois ans qui suivent une cyberattaque.** L'insécurité numérique et donc un facteur d'insécurité économique.

[29] *Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022,* étude du cabinet en recherche et conseil économique Asterès, juin 2023.

Retour d'expérience : la cyberattaque contre le CIG Grande couronne

Le Centre interdépartemental de gestion (CIG) Grande couronne de la région d'Île-de-France, établissement public local à caractère administratif, accompagne au quotidien plus de 1 000 collectivités territoriales et établissements des départements des Yvelines, de l'Essonne et du Val d'Oise et suit près de 45 000 agents.

À la fin du mois de janvier 2022, l'équipe du CIG détecte une intrusion dans ses systèmes d'information. Alerté, son directeur général, en liaison avec le président, prend la décision de couper immédiatement tous les services et moyens de communication du CIG, rompant les liens entre les agents mais aussi entre l'organisation et ses membres. Cette décision constitue le point de départ de ce que le directeur général qualifie de « course contre le temps » pour gérer quatre défis auxquels il a fallu faire face simultanément :

- **Enjeux techniques :** qualification de la cyberattaque, de son origine, de son périmètre, de la portée réelle de l'attaque et des « dégâts » sur les systèmes d'information du CIG ;
- **Enjeux juridiques :** déclarations administratives et dépôts de plainte auprès des autorités compétentes, chacune disposant de délais différents, le tout privés des moyens de communication de la structure ;
- **Enjeux de communication :** gestion de la relation avec le conseil d'administration du CIG mais aussi avec ses adhérents, entre rupture de communication et craintes de rupture de services essentiels pour les collectivités membres (gestion de paie, suivi de carrière, organisation des concours administratifs, etc.) ; mais aussi gestion des sollicitations de la presse, sans disposer d'informations véritablement fiables le temps nécessaire aux investigations techniques ;
- **Enjeux managériaux :** lors de son audition, le directeur général du CIG a salué le grand professionnalisme et l'engagement des agents, à tous les niveaux de responsabilité ; des agents ont cependant très mal vécu cet épisode et ont ressenti angoisse, sentiment de culpabilité, certains tombant en *burn-out* ; une cellule psychologique a été mise en place.

Le CIG a reçu une aide de premier niveau de la CNIL et de l'ANSSI, notamment pour gérer les demandes d'information des membres et mobiliser un prestataire qualifié pour effectuer un diagnostic d'urgence, en complément de sa propre équipe technique : il a été très difficile de faire patienter toutes les parties-prenantes le temps d'obtenir le rapport d'expertise, soit environ un mois et demi. Le président et le directeur du CIG ont échangé avec les collectivités et établissements adhérents pour les rassurer, les accompagner, et leur expliquer la situation. Ce choix d'une communication « transparente » s'est avéré fructueux puisqu'aucune collectivité territoriale ne s'est désaffiliée du CIG.

L'exécutif et la direction du CIG ont tiré trois conclusions principales de cette crise :

- **L'organigramme de l'équipe a été modifié pour intégrer une « cellule cyber »** réunissant le DSI, le RSSI et le délégué à la protection des données personnelles (DPO), sous la présidence du directeur général : aucun de ces acteurs ne dépendant d'un autre, ce cadre favorise l'émulation et permet à l'organisation de s'inscrire dans une démarche d'amélioration continue. Le directeur général explique avoir voulu envoyer un signe managérial fort de responsabilité et de prise en compte du sujet au plus haut niveau.
- **Une nouvelle approche du projet d'établissement :** un travail collectif sur une cartographie des risques et des plans de cessation, continuité et reprise d'activité, associé à une définition claire des responsabilités, a permis d'accompagner la transition d'un modèle basé sur la résolution de problèmes à la gestion de risques. La direction expérimente depuis lors un « jour sans connexion » avec tous les agents du CIG pour favoriser la continuité d'activité en cas de coupure réseau.
- **La stratégie de sécurisation du système d'information a été renforcée :** authentification, segmentation des données, multiplication des sites sur lesquels elles sont hébergées (augmente l'exposition au risque, mais en diminue l'impact en réduisant le nombre simultanément concernées par une cyberattaque). Le CIG consacre désormais 10 % de son budget informatique annuel à la sécurité (contre 2 à 3 % auparavant).

Le CIG, accompagné par l'ANSSI, structure un service d'accompagnement de ses adhérents et a édité un guide[30] pour partager son expérience avec d'autres collectivités, pour les aider à prévenir et gérer leur exposition au risque numérique.

[30] *Cyberattaque - Gérer la crise, se reconstruire et se protéger*, Centre interdépartemental de gestion Grande couronne de la région d'Île-de-France, juillet 2023.

1.6 L'assurance contre le risque cyber : une solution sous conditions

Les entreprises se sont naturellement tournées vers les sociétés d'assurance qui ont développé une gamme de produits destinés à atténuer les conséquences d'une cyberattaque réussie. Il est certain que l'augmentation croissante du nombre de cyberattaques, tout comme l'élargissement de leurs cibles potentielles, nourrissent **un marché en plein développement, dans un contexte où la puissance publique et les grandes entreprises accroissent leurs exigences en matière de cybersécurité vis-à-vis de leurs prestataires et sous-traitants**. Un changement de doctrine s'opère en effet à mesure que l'évolution des technologies et des usages remet en cause les modèles antérieurs de protection numérique, dans lesquels chaque acteur était responsable de son propre périmètre : la politique dite *« zero trust »* consiste au contraire à réduire la « confiance implicite » entre les contractants et à s'assurer que chaque échange soit bien contrôlé et sécurisé[31].

Les compagnies d'assurance proposent aujourd'hui des contrats apportant des garanties qui répondent aux multiples dimensions des conséquences d'une cyberattaque, principalement :

- des prestations d'accompagnement de la gestion de crise afin de bloquer la cyberattaque et d'en limiter les conséquences,
- les dépenses liées à la responsabilité de l'entreprise en cas d'atteinte à la protection des données personnelles, et notamment en cas de poursuites judiciaires intentées par des tiers estimant avoir subi des dommages du fait de l'insuffisance de protection du système informatique de l'entreprise attaquée,
- les dommages aux données et aux systèmes d'information causés par une cyberattaque quelle qu'en soit la forme : perte d'exploitation, frais d'experts informatiques, frais de restauration des systèmes et des données, etc.,
- la perte découlant du transfert de fonds à la suite d'une intrusion dans le système d'information sans intervention de tiers,
- le paiement d'une rançon suite au cryptage des données, mais également les frais liés au recours d'une entreprise spécialisée dans la négociation avec des cybercriminels.

Les fluctuations importantes des primes versées par les premières entreprises souscriptrices de ces nouveaux contrats ont conduit l'Assemblée nationale, dans un rapport[32] publié fin 2021, **à proposer des mesures de régulation du secteur** avec une vigilance particulière pour les TPME. Si le rapport recommandait l'autorisation de couverture et de prise en charge des amendes administratives par les assureurs, il proposait *« d'inscrire dans la loi l'interdiction de garantir, couvrir ou d'indemniser la rançon »* exigée après une cyberattaque pour *« se porter davantage vers la prévention, l'accompagnement et l'assurance des conséquences pour une entreprise ».* Selon la présidente du groupe d'études « Assurances » de l'Assemblée, *« le paiement des rançons alimente la cybercriminalité et rien ne garantit que la rançon payée soit un gage de retour à la situation initiale ».*

Cette option n'a pas été retenue par le législateur qui, sans se prononcer sur cette proposition, a néanmoins clarifié les modalités d'intervention des assureurs dans le sens du rapport parlementaire : **la loi « LOPMI » adoptée tout début 2023[33] crée une nouvelle obligation, à la charge de l'assuré, qui conditionne le versement d'une indemnité par exécution d'un contrat d'assurance à un dépôt de plainte dans les 72 heures après la connaissance de la cyberattaque.** Cette loi durcit par ailleurs les peines encourues par les cybercriminels. Si cette nouvelle disposition reste discutée, notamment parce qu'elle fait peser une nouvelle responsabilité sur l'entreprise victime et ne répond pas aux interrogations portées spécifiquement sur les conséquences du paiement d'une rançon, **elle facilite, néanmoins, un meilleur signalement des**

[31] Audition de Bernard GIRY, 5 septembre 2023.

[32] *La cyber-assurance*, rapport conduit par Valéria FAURE-MUNTIAN, députée de la Loire et présidente du groupe d'études « Assurances » de l'Assemblée nationale, octobre 2021.

[33] L'art. 5 de la loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (JORF du 25 janvier 2023) introduit un nouvel article L12-10-1 au code des assurances, rédigé comme suit : *« Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime. Le présent article s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle. »*

cyberattaques aux forces de l'ordre et aux autorités compétentes, participant ainsi à leur meilleure connaissance et à l'adoption de mesures de protection adaptées.

Ces positions contrastées se sont d'ailleurs exprimées dans les auditions menées par le Ceser dans le cadre de ce rapport. Pour certains, contracter une assurance contre le risque cyber peut s'avérer vertueux si la démarche est associée à un diagnostic de cybersécurité avant la signature du contrat, participant ainsi à la sensibilisation des chefs d'entreprise. La question du plafond de dépenses maximum couvert par l'assurance et, partant, du montant de la prime, est plus sensible : il faut bien identifier et quantifier les risques pour estimer les coûts de remédiation, et déterminer si l'offre proposée est adaptée à l'entreprise concernée, et à son risque de pérennité en cas de cyberattaque.

L'enjeu d'amélioration de l'offre reste prégnant, *« notamment en limitant les clauses d'exclusion et en adaptant le processus de souscription à la taille de l'entreprise »*[34], selon Philippe COTELLE, président de la commission « cyber » de l'Association pour le management des risques et des assurances de l'entreprise (AMRAE). Dans un avis[35] adopté en avril 2022, le Conseil économique, social et environnemental (CESE) recommandait pour sa part de :

- *« rendre accessible (tant pour les particuliers que pour les professionnels et les entreprises) une couverture assurantielle abordable portant sur les garanties essentielles »* ;
- *« créer une branche d'assurance dédiée au cyber »* ainsi qu'*« un contrat cyber « socle » destiné aux TPE/PME proposant les garanties essentielles telles que l'assistance au redémarrage de l'activité, les pertes d'exploitation et la conformité réglementaire ».*

Selon les données collectées par l'AMRAE, il est possible d'évaluer le montant des primes sur le segment des TPE/PME, catégorie d'entreprises qui dispose de moins de moyens pour se protéger en dehors de l'assurance et pourtant la moins bien assurée :

	Nombre d'entreprises assurées en 2022 (évolution / 2021)	**Volume des primes collectées en 2022, en M€** (évolution / 2021)	**Taux de prime rapporté au CA couvert, en %** (évolution / 2021)	**Montant moyen de la prime en 2022, en euros**
Ent. de taille moyenne (CA de 10 à 50 M€)	492 (+ 53 %)	4,50 (+ 84 %)	0,40% (+ 22 %)	**9 150**
Petites entreprises (CA de 2 à 10 M€)	624 + 24 %	2,15 - 36 %	0,57% - 13 %	**3 450**
Micro-entreprises (CA inférieur à 2 M€)	7 684 NS	3,89 + 208 %	0,16 % - 51 %	**510**
Totaux TPE/PME	8 800	10,54		
Totaux marché global	9 672	357,7		

CA = chiffre d'affaires ; M€ = million d'euros | Source : Enquête *LUCY (LUmière sur la CYberassurance)*, 3ème édition, Association pour le management des risques et des assurances de l'entreprise (AMRAE), mai 2023.

Les données de l'AMRAE font ressortir la modicité de la prime moyenne annuelle d'un contrat d'assurance contre le risque cyber, rapportée au chiffre d'affaires de l'entreprise : de l'ordre de 500 euros annuels pour une petite entreprise.

En conclusion, comme le pointait le rapport du groupe d'études de l'Assemblée nationale : *« un équilibre doit être recherché en associant une demande sensibilisée, alerte et soucieuse de sa sécurité, avec une offre cohérente, adaptée et suffisamment compétitive pour convaincre les entreprises »*[36]. Aujourd'hui, il importe que les petites entreprises puissent mesurer leur risque de trésorerie, qui peut être gravement affectée par les conséquences d'une cyberattaque, et puissent mettre en œuvre des solutions pour la protéger.

[34] Propos rapportés par Raphaële KARAYAN pour *l'Usine digitale* : Assurance cyber : les PME s'assurent plus qu'avant, et elles vont bientôt le regretter, article publié le 24 mai 2023.
[35] *Climat, cyber, pandémie : le système assurantiel mis au défi des risques systémiques*, avis du Conseil économique, social et environnemental (Cese) N°2022-007, adopté le 13 avril 2022.
[36] *La cyber-assurance*, octobre 2021, op. cit.

Selon la formule utilisée par les experts entendus en audition par le Ceser : aujourd'hui, il n'est plus question de savoir « si » une entreprise sera victime d'une cyberattaque, mais « quand ». Pourtant, même informées et sensibilisées, *« on constate peu d'engagement opérationnel des entreprises »*[37], comme des associations et des petites collectivités territoriales[38] : les défis sont multiples et les solutions pour y répondre sont pour la plupart en cours de structuration.

[37] Audition d'Anne-Sophie COLLÉAUX, 30 juin 2023.
[38] Cybersécurité : les structures mutualisantes peinent à enrôler les maires des petites communes, *La Gazette des Communes*, publié le 6 octobre 2023.

2 Au croisement d'enjeux multiples, la cybersécurité est une responsabilité collective

2.1 Un enjeu de conformité à une réglementation mouvante et complexe

Depuis les lois fondatrices du droit des nouvelles technologies de l'information et de la communication en 1978 et 1988[39], le cadre normatif dans lequel doivent s'inscrire les acteurs économiques connaît des évolutions permanentes au regard du besoin d'adaptation rapide de la réglementation aux nouvelles formes que prend le risque numérique. Les experts entendus en audition par le Ceser se rejoignent sur **la difficulté que rencontrent les chefs d'entreprise pour comprendre la nature règlementaire de chaque nouvelle disposition, les exigences attendues fonction de son activité et donc l'effort attendu pour se mettre en conformité.**

Les cyberattaques ne connaissent pas les frontières des États : de fait, l'Union européenne est devenue la principale prescriptrice en la matière pour harmoniser les pratiques de lutte contre la cybercriminalité des États membres. L'Union s'est dotée dès 2004[40] d'une Agence européenne pour la cybersécurité (ENISA) dont le mandat a été réaffirmé par le *Cybersecurity Act*[41] adopté en 2019. Elle est aujourd'hui à la fois à l'origine de schémas européens de certification de cybersécurité afin de renforcer la confiance dans les produits, services et processus numériques, et un espace de coopération entre les autorités et agences nationales en charge de la sécurité numérique, à l'instar de l'ANSSI pour la France.

La réglementation européenne ne concerne pas que les États membres mais crée un cadre de responsabilités pour les acteurs économiques des pays de l'Union. Les textes se multiplient dans des délais resserrés. Parmi ceux-ci :

- Le Règlement général sur la protection des données (RGPD)[42], adopté en avril 2016, a considérablement renforcé les obligations de tous les organismes publics et privés établis sur le territoire de l'Union (incluant les entreprises, les associations, les collectivités, etc.), pour garantir la protection des données qu'elles traitent pour leur compte ou pour un tiers.
- La première directive européenne sur la sécurité des réseaux et des systèmes d'information (SRI)[43], adoptée en juillet 2016, a établi des obligations en matière de sécurité numérique pour les opérateurs des secteurs stratégiques (transports, énergie, santé, finance, etc.), créant l'obligation de notifier à l'autorité nationale compétente les incidents de sécurité numérique qu'ils rencontrent. Ce texte a déjà fait l'objet d'une révision : annoncée par la Commission européenne en décembre 2020 et adoptée en novembre 2022, la directive dite « SRI/2 »[44] élargit ces obligations à un plus grand nombre de secteurs et vise à renforcer la régulation des entreprises par l'autorité nationale compétente. Alors que les États membres doivent transposer cette directive européenne en droit national d'ici l'automne 2024, l'ANSSI a déjà indiqué qu'*« elle s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs qui seront désormais régulés […], des administrations de toutes tailles et des entreprises allant des PME aux groupes du CAC40. Les principaux critères d'intégration ont été définis au niveau européen : il s'agit*

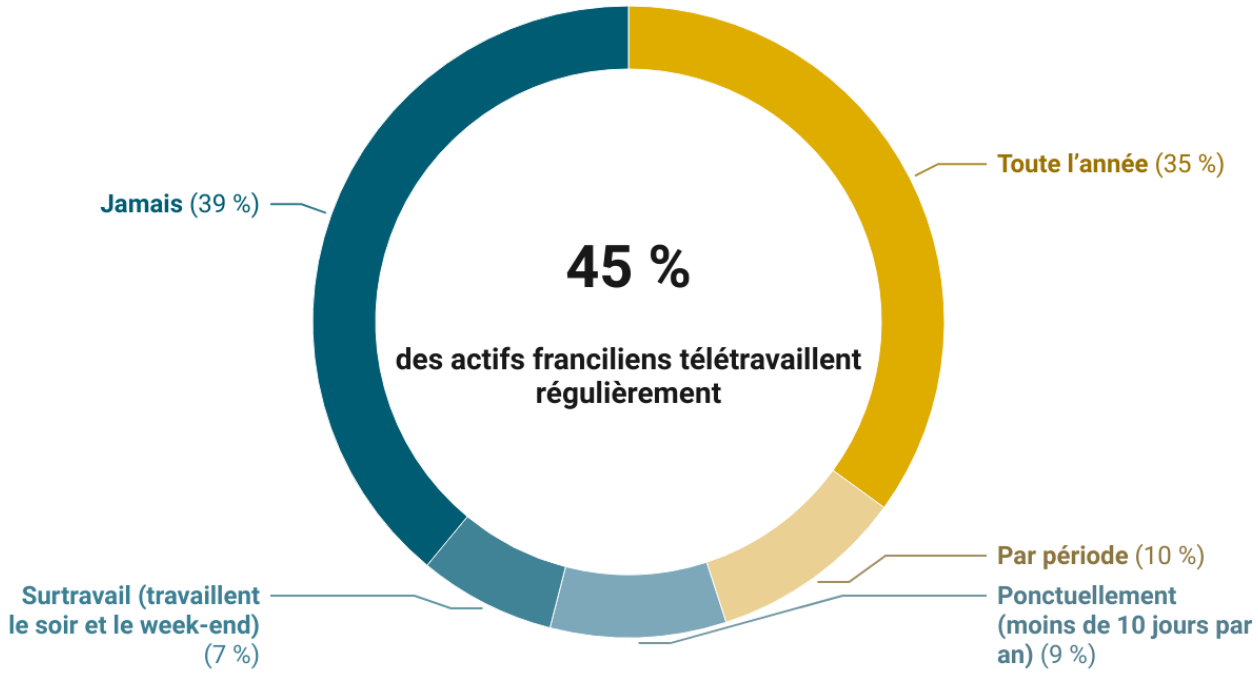
[39] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « informatique et libertés », qui acte la création de la CNIL, introduit la notion de « système de traitement automatisé de données » et les obligations du responsable du traitement quant à la garantie de la sécurité des données ; puis la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite « loi Godfrain », citée précédemment (cf. note de bas de page n° 6).
[40] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, JOUE du 13 mars 2004.
[41] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'Enisa (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité), JOUE du 7 juin 2019.
[42] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOUE du 4 mai 2016.
[43] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JOUE du 19 juillet 2016.
[44] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, JOUE du 27 décembre 2022.

principalement du nombre d'employés, du chiffre d'affaires et de la nature de l'activité réalisée par l'entité. »[45]

- Le règlement « DORA » pour la résilience opérationnelle du numérique[46], adopté en décembre 2022, vise quant à lui à renforcer la sécurité des systèmes numériques des entreprises du secteur bancaire et assurantiel, qui doivent désormais répondre à des tests approfondis pour vérifier s'ils sont bien préparés face aux attaques informatiques.

2.2 Un enjeu d'adaptation aux nouvelles pratiques du travail et de la consommation

Le développement du télétravail consécutif à la crise sanitaire de la Covid-19 est prégnant en Île-de-France. Selon l'Ifop, les salariés français sont aujourd'hui 34 % à télétravailler[47]. Mais l'Île-de-France marque sa différence : d'après le dernier *Baromètre des Franciliens* réalisé par l'Ipsos et l'Institut Paris Région[48], 45 % des actifs franciliens ont travaillé à distance en 2023, en moyenne 2,1 jours par semaine. Ils n'étaient que 20 % avant la pandémie.



Source : *Baromètre des Franciliens – Édition 2023*, Institut Paris Région, d'après une enquête réalisée par Ipsos, 12 octobre 2023.

De nombreux chefs d'entreprise manifestent leur inquiétude sur leur responsabilité et celles de leurs salariés alors que le développement du *flex-office*, du télétravail ou du travail en tiers-lieu rend plus difficile la sécurisation de l'accès aux données de l'entreprise. Le bouleversement des cadres professionnels « traditionnels » réclame des évolutions technologiques devenues indispensables (outils de visioconférence, de partage instantané d'informations, informatique en nuage, etc.) qui pourraient accroître la surface à défendre, elle-même déjà sujette à l'inventivité des cybercriminels.

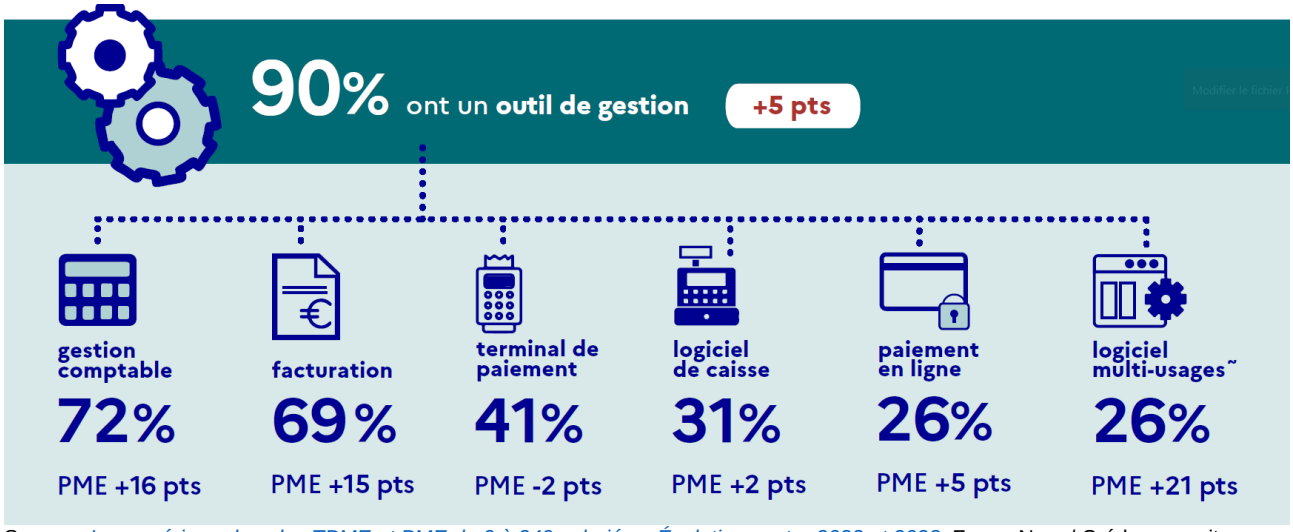
Les grandes entreprises et administrations réagissent en équipant leurs collaborateurs de terminaux sécurisés, mais les plus petites structures n'en ont pas forcément les moyens. Et, dans la plupart des cas, l'utilisation d'un ordinateur ou d'un réseau public ou personnel pour accéder au système professionnel, l'utilisation d'une imprimante familiale, la porosité des usages professionnels et personnels sur les mêmes terminaux, etc. sont autant de fenêtres de vulnérabilités.

[45] Source : site internet de l'Anssi, consulté le 24 octobre 2023.
[46] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, JOUE du 27 décembre 2022.
[47] Norme Ifop de climat social, enquête menée en octobre 2022 auprès d'un échantillon représentatif de 1300 salariés, citée par *Le Journal du Dimanche*, Télétravail : l'Île-de-France championne du travail à distance, 21 janvier 2023.
[48] *Baromètre des Franciliens – Édition 2023*, Institut Paris Région, d'après une enquête réalisée par Ipsos, 12 octobre 2023.

Parmi les évolutions sources d'inquiétude, de nombreux chefs d'entreprise évoquent aussi **la numérisation d'un nombre croissant de procédures et la mise en place de la facturation électronique,** obligatoire depuis le 1er janvier 2021 pour la transmission des factures destinées aux organismes publics et dont la généralisation, initialement prévue au 1er juillet 2024, est reportée à une date qui sera décidée dans le cadre de la loi de finances pour 2024 : de nombreuses TPE/PME sont contraintes de recourir à des prestations nouvelles externalisées pour s'adapter à ces obligations – ce qui ouvre un nouveau champ de risque potentiel.

Quant aux nouvelles habitudes de consommation, si elles dynamisent tout à la fois le commerce de proximité et le e-commerce, **le développement du paiement dématérialisé sans-contact constitue aussi une source d'inquiétude pour de nombreux commerçants.** Signalons qu'outre les démarches entreprises par la Banque de France (cf. encadré p. 8) et l'Observatoire de la sécurité des moyens de paiement (OSMP, cf. p. 32), la Commission européenne prépare une règlementation-cadre[49] pour imposer de nouveaux standards minimums de sécurité aux fabricants d'objets connectés, en les obligeant, par exemple, à fournir des mises à jour permettant de remédier aux vulnérabilités de ces produits tout au long de leur cycle de vie.

Signe de ces évolutions, **les TPME connaissent ainsi un « rattrapage » rapide d'équipement en solutions de gestion, de facturation et de paiement :**



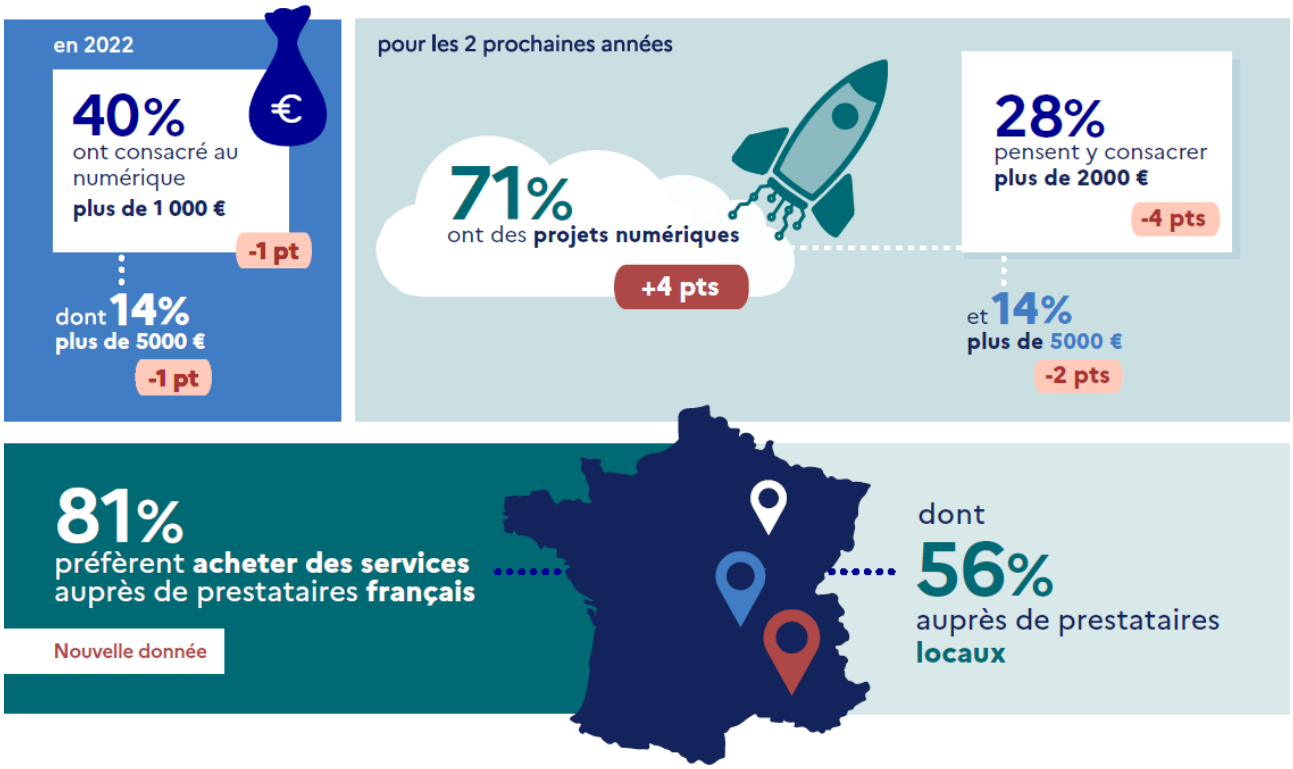
Source : *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023,* FranceNum / Crédoc, op. cit.

Ces inquiétudes sont relayées par les organisations professionnelles. On peut par exemple citer la réalisation, par la CCI de Paris en partenariat avec la préfecture de Police de Paris, de fiches[50] à l'intention des commerçants, hôteliers, restaurateurs et professionnels du tourisme parisiens, qui intègrent les différentes formes de *« cyber-atteintes »* dont ils peuvent être victimes en les invitant, via un système de QR-code, à entrer en contact avec les services de police compétents.

2.3 Un enjeu de lisibilité et d'accessibilité de l'offre de services aux entreprises

À mesure que la prise de conscience progresse, **un plus grand nombre d'entreprises prévoit de réaliser *« des projets numériques »*** (qui incluent des mesures de protection contre le risque numérique) dans les deux prochaines années (71 % des TPME en 2023, soit une augmentation de + 4 points par rapport à 2022). Dans un contexte économique inflationniste, **ces mêmes envisagent cependant de réduire leurs dépenses** pour les mettre en œuvre : 44 % des TPME prévoient de dépenser plus de 1 000 euros (- 3 points), 28 % plus de 2 000 € (- 4 points) et seulement 14 % plus de 5 000 euros (- 2 points).

[49] Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques *(European Cyber Resilience Act),* 15 septembre 2022.
[50] Disponibles sur le portail internet de la Cci Paris.



Source : *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023,* FranceNum / Crédoc, op. cit.

Dans le cadre d'une mission[51] confiée en novembre 2022 par le ministre délégué chargé du Numérique, le Campus Cyber (cf. p. 22) a établi une première cartographie qui présente le *« millefeuille[52] »* auquel fait face une PME pour gérer sa cybersécurité : d'une part, l'offre est de plus en plus importante, ce qui complique la lecture du marché pour un dirigeant d'entreprise ; d'autre part, il y a énormément d'offres dans le domaine de la sensibilisation et du diagnostic, mais beaucoup moins sur l'accompagnement de la gestion d'une cyberattaque et la remédiation des systèmes d'information attaqués.

Dès lors, les chefs d'entreprises qui entrent dans une démarche de cyberprotection sont nombreux à se questionner : les offres proposées sur le marché répondent-elles aux besoins des entreprises, en particulier des TPME ? quels sont les prestataires « de confiance » ? que valent les « labels » qui se multiplient ? **Des efforts doivent encore être faits pour structurer et faire connaître une offre adaptée aux acteurs économiques selon leur taille et leur niveau d'exposition au risque.**

Selon le consortium francilien Cybiah[53] (cf. p. 34), les principales difficultés que rencontrent les entreprises en recherche de prestataires de services numériques sont liées à :

- L'absence de référentiel partagé des acteurs du diagnostic : le consortium Cybiah veut participer à répondre à ce besoin en travaillant, avec ses homologues sur le territoire national, à un référentiel commun aux prestataires de services de sécurité numérique, afin d'adresser une offre lisible et claire à même de répondre aux entreprises d'une région à l'autre ;
- Des outils d'autoévaluation insuffisamment adaptés aux TPME : comment qualifier un problème qu'on cerne mal ?
- Une offre de formation en sécurité informatique insuffisante ou peu accessible ;
- Une approche parfois trop *« brusque »,* ou insuffisamment individualisée du sujet, qui demande *« une réponse proportionnée, adaptée et échelonnée dans le temps » :* pour Cybiah, le diagnostic initial doit aussi montrer *« ce qui va bien »* et comment les entreprises peuvent encore améliorer leurs processus à partir de l'existant et non pas d'un *« objectif-cible à atteindre »* qui serait le même pour toutes les entreprises ;

[51] Jean-Noël Barrot missionne le Campus Cyber pour assurer la protection des PME, *cybersecurite-solutions.com*, 28 novembre 2022
[52] Audition d'Anne-Sophie COLLÉAUX, 30 juin 2023.
[53] Audition d'Anne-Sophie COLLÉAUX, 30 juin 2023.

- Un manque de coordination : Cybiah plaide pour un raisonnement en *« chaîne de services »* auprès des entreprises, ce qui suppose de développer l'interconnexion entre les corps de métier et la transversalité des interventions.

Pour Cybiah, la priorité est bien d'accompagner chaque entreprise afin qu'elle puisse se tourner vers le marché de manière éclairée, dans le respect du droit de la concurrence, à partir d'un état des lieux de ses besoins qui lui permette d'appeler les bonnes spécialités pour y répondre. L'ANSSI plaide aussi pour une approche progressive et inscrite dans le temps : *« tous les problèmes de sécurité informatique ne se résolvent pas en sortant son chéquier en une seule fois »*[54] : l'entreprise, selon ses besoins, doit prévoir un budget ad hoc, le sanctuariser pour actualiser sa stratégie de sécurité et la développer. Il n'est pas forcément besoin, selon son activité, d'un budget conséquent ; mais il faut accepter d'avancer progressivement et rechercher les mutualisations, notamment pour les petites structures qui disposent de ressources propres limitées.

Plusieurs initiatives sont prises au niveau national et régional pour éclairer la décision des chefs d'entreprise.

Pour FranceNum, le ou les labels dont bénéficie un prestataire de services numériques, l'appartenance à un réseau professionnel tout comme la pertinence de ses références clients sont des indicateurs de qualité. Aussi **la plateforme francenum.gouv.fr recense-t-elle ces éléments pour faciliter la recherche de partenaires.**

L'ANSSI tient à jour une liste de produits, services et prestataires dont la conformité aux prescriptions européennes et nationales de sécurité numérique est attestée[55]. CyberMalveillance (cf. p. 30), en partenariat avec les principales organisations professionnelles du secteur et l'Afnor, a initié **le label ExpertCyber**[56] certifiant *« les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients ».*

Toujours selon FranceNum, *« quatre entreprises sur cinq (81 %) déclarent vouloir privilégier un prestataire français pour acheter des services* [numériques], *dont 56 % un prestataire local proche géographiquement de l'entreprise »*[57]*.* Pour l'achat de logiciels, la proportion d'entreprise déclarant préférer un acteur français atteint 65 %. Cette préoccupation rejoint celle de nombreux acteurs publics pour accompagner la croissance d'un écosystème « souverain » de la cybersécurité, à même de répondre aux enjeux des acteurs locaux, tout en tenant compte des contraintes imposées par la règlementation sur la commande publique. La Région Île-de-France a inscrit cet objectif dans son SRDEII 2022-2028 : *« Développer un écosystème francilien de prestataires de services certifiés/labellisés et répondant aux besoins des entreprises de toutes tailles, en particulier des TPE et PME »*[58]*.*

Outre les aides régionales versées directement à des entreprises des secteurs d'activité *« du numérique et de l'industrie de la donnée »,* inscrits parmi les *« filières stratégiques »* régionales au sens du SRDEII, **la Région Île-de-France a publié un appel à manifestation d'intérêt**[59] **en octobre 2023 pour engager un référencement des prestataires franciliens de réponse à cyber incident**. Ce référencement, organisé dans le cadre du projet de « cybercaserne » régionale (cf. p. 39), s'effectue sur la base du volontariat et il est gratuit pour les entreprises prestataires de service. Le dossier de référencement doit indiquer les effectifs du prestataire, les métiers de la cybersécurité qu'il propose (analyste, gestionnaire de crise, etc.) et le niveau d'expérience de ses collaborateurs

[54] Guillaume CRÉPIN, délégué territorial Île-de-France de l'Agence nationale de la sécurité des systèmes d'information (Anssi), entendu en audition par la commission Développement économique du Ceser Île-de-France le 16 mai 2023.
[55] Liste disponible sur le site internet de l'Anssi.
[56] Présentation du label sur le site internet de CyberMalveillance.
[57] *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023,* FranceNum / Crédoc, op. cit.
[58] Délibération n° CR 2022-029 - Schéma régional de développement économique d'innovation et d'internationalisation d'Île-de-France 2022-2028 (axe 1, sous-axe 1.2 : *« Protéger les TPE, PME et ETI contre l'exposition au risque grandissant de cyber-attaque »),* adoptée par le Conseil régional le 19 mai 2022.
[59] Description complète de l'appel à manifestation d'intérêt sur le site internet de la Région Île-de-France, consulté le 26 octobre 2023.

(junior, confirmé ou senior). En cohérence avec les questionnements des chefs d'entreprise, l'inscription sur la liste des prestataires référencés est subordonnée à :

- leur qualification par l'ANSSI ou leur détention du label « ExpertCyber » (cf. p. 21),
- et la signature d'une « Charte de fonctionnement » par laquelle les entreprises prestataires de service retenues s'engagent à « la pertinence et l'adéquation de l'offre commerciale » et l'acceptation d'une « évaluation » par le bénéficiaire (devenu client).

2.4 Un enjeu de structuration de la filière professionnelle

Toutes les sources rejoignent le constat dressé en 2020 par l'ANSSI dans son premier *Panorama des métiers de la cybersécurité* : *« Les spécialistes en cybersécurité sont aujourd'hui des perles rares : l'intérêt pour la filière est grandissant, mais le vivier de talents peine encore à répondre à l'importance des besoins. Et ces profils sont d'autant plus difficiles à dénicher que le champ des missions et compétences de la cybersécurité est vaste, complexe, hétérogène. Soit, difficile à appréhender pour qui n'y est pas familier. Dans ce contexte, la formation et le recrutement sont des enjeux fondamentaux. »*[60] La filière professionnelle de la cybersécurité, parmi les métiers du numérique, est particulièrement jeune : ainsi, 45% des professionnels de la cybersécurité interrogés par l'ANSSI en 2021 avaient moins de cinq ans d'ancienneté[61].

L'Île-de-France, qui réunit de nombreux centres de formation, entreprises du numérique et pôles de recherche, est la première région française pour la filière de la cybersécurité : elle concentre 54 % des professionnels[62] et 21 % des offres de formation[63] de la sécurité numérique. Le territoire compte sur plusieurs pôles d'excellence en particulier à Paris, dans les Hauts-de-Seine autour du quartier de La Défense et dans l'Essonne avec le campus Paris-Saclay.

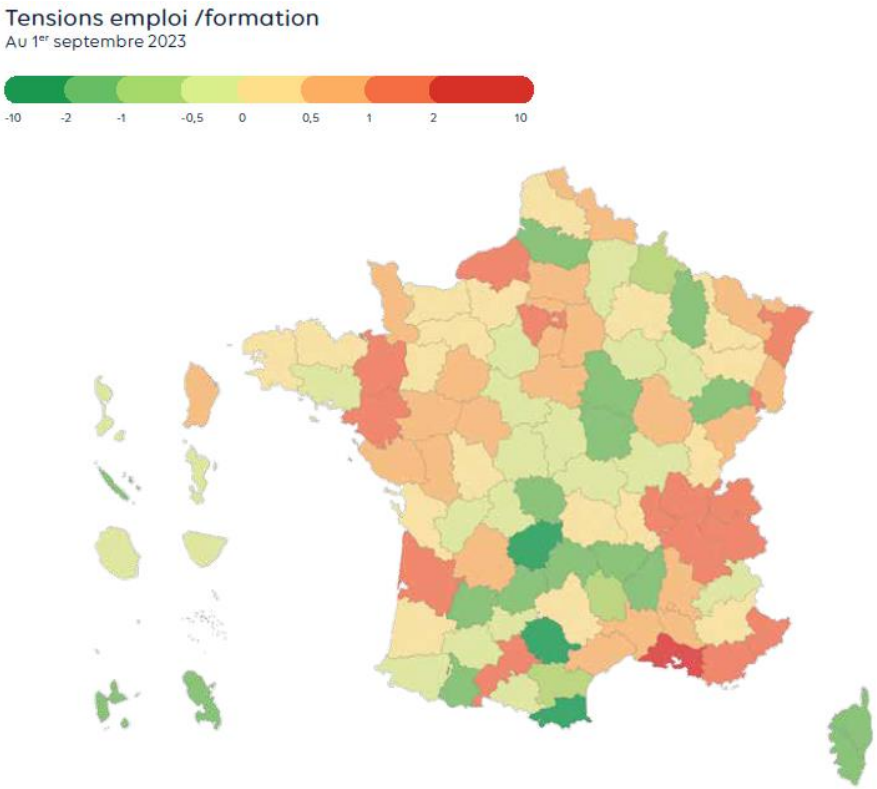
Le territoire francilien accueille **le Campus Cyber, *« lieu totem »* de la cybersécurité nationale.** Le projet, financé dans le cadre de la Stratégie nationale d'accélération pour la cybersécurité[64] et inauguré en février 2022, est issu d'un partenariat public/privé (l'État est actionnaire à 39% via l'Agence des participations). L'ambition[65] du Campus Cyber est de rassembler en un seul lieu les principaux acteurs nationaux, européens et internationaux du secteur pour renforcer notre capacité collective à maîtriser le risque numérique : entreprises (grands groupes et PME), services de l'État, organismes de formation, acteurs de la recherche et associations. Plus de 250 organisations sont aujourd'hui parties-prenantes du projet (membres, partenaires ou résidents). Le Campus Cyber fait de la formation initiale et continue un de ses piliers d'action pour soutenir la montée en compétence de l'écosystème de la cybersécurité et proposes des groupes de travail pour animer cet écosystème dans une visée prospective (par ex. : développer l'attractivité des métiers cyber pour les femmes)[66].

Malgré tous ces atouts, *« la région connaît des besoins de recrutement importants et croissants et cette tendance risque de s'accentuer pendant les prochaines années »*[67], selon le diagnostic territorial conduit par le Conseil régional dans la phase d'élaboration de son SRDEII 2022-2028.

Si l'année 2023 constate une chute des offres d'emploi en Île-de-France dans les métiers du numérique, sous l'effet de la conjoncture économique, d'une part, et d'un rééquilibrage entre territoires au niveau national, d'autre part, **la filière reste considérée « en tension » au regard des besoins en compétences et en formation : ainsi 57 % des recrutements dans les métiers du numérique (toutes spécialités confondues) sont jugés difficiles**[68]. S'agissant des métiers de

[60] *Panorama des métiers de la cybersécurité – Édition 2020,* Anssi avec Syntec Numérique, octobre 2020.
[61] *Les profils de la cybersécurité – Enquête 2021*, Observatoire des métiers de la cybersécurité (Anssi avec l'Afpa et la délégation générale à l'emploi et à la formation professionnelle du ministère du Travail, de l'Emploi et de l'Insertion), septembre 2021.
[62] *Les profils de la cybersécurité – Enquête 2021*, Observatoire des métiers de la cybersécurité, septembre 2021, op.cit.
[63] Selon les données au 1er octobre 2023 mises en ligne par l'Observatoire GEN_SCAN (GIP Grande École du Numérique), consultées le 26 octobre 2023.
[64] *Dossier de presse : Cybersécurité, faire face à la menace : la stratégie française*, Gouvernement, 18 février 2021.
[65] Voir aussi le *Manifeste* du Campus Cyber.
[66] Audition d'Anne-Sophie COLLÉAUX, 30 juin 2023.
[67] Délibération n° CR 2022-029 - Schéma régional de développement économique d'innovation et d'internationalisation d'Île-de-France 2022-2028 (axe 1, sous-axe 1.2 : *« Protéger les TPE, PME et ETI contre l'exposition au risque grandissant de cyber-attaque »),* adoptée par le Conseil régional le 19 mai 2022.
[68] *Rentrée 2023 : tendances de l'emploi et de la formation au numérique en France,* 2ème édition, rapport de l'Observatoire GEN_SCAN, GIP Grande École du Numérique, 1er octobre 2023.

la cybersécurité, les services d'accompagnement de la gestion d'une cyberattaque, en particulier, font aujourd'hui particulièrement défaut au regard des besoins et de la demande selon Cybiah, (cf. p. 34). En prospective, l'essor des nouvelles technologies liées au déploiement de la 5G et de l'internet des objets (*Internet of Things* ou IoT), qui nécessitent une double compétence en télécom et en cybersécurité, représenterait un vivier de 100 000 emplois à l'horizon 2027 en France[69].



Cartographie des tensions emploi/formation au 1er septembre 2023 pour la famille de métiers « Sécurité, cloud, réseau et télécom », issue du rapport Tendances de l'emploi et de la formation au numérique en France, GEN_SCAN, 1er octobre 2023, op. cit.

Compétente pour la formation et l'insertion professionnelle des jeunes et des demandeurs d'emploi, **la collectivité régionale doit maintenir un haut niveau de vigilance pour soutenir l'attractivité des métiers et des formations de la filière (ainsi que leurs débouchés),** notamment dans le cadre de l'agence Oriane, au regard des enjeux lourds de la cybersécurité pour la souveraineté économique régionale. Le soutien apporté par la Région à la création d'un Campus des métiers et des qualifications « Métiers de la sécurité »[70] (incluant un volet cybersécurité), en partenariat avec la Région académique et l'Académie de Versailles, participe à cet effort qui doit s'inscrire dans le temps.

Dans ce contexte hyperconcurrentiel, les TPME, les collectivités et les associations sont à la peine. Le secteur public en particulier, peine à attirer les talents, compte tenu des règles particulières qui encadrent l'emploi et la rémunération dans la fonction publique[71]. 73 % des professionnels de la cybersécurité exercent dans le secteur privé contre seulement 22 % dans le secteur public, 3 % en indépendant ou auto-entrepreneur et 1 % dans le milieu associatif (1 % non précisé)[72]. Ces difficultés constituent *« une puissante incitation à externaliser la gestion des bases de données et, plus globalement, la cybersécurité de l'entreprise »*[73].

[69] *Étude sur les besoins en compétences, emplois et formations de la 5G en France*, Observatoire prospectif des métiers du numérique, de l'ingénierie, des études et du conseil et des métiers de l'événement (OPIIEC), juin 2022.
[70] La présentation du CMQ est disponible sur le site internet de la Région Île-de-France, consulté le 26 octobre 2023.
[71] Audition de Bernard GIRY, 5 septembre 2023.
[72] *Les profils de la cybersécurité – Enquête 2021*, Observatoire des métiers de la cybersécurité, septembre 2021, op.cit.
[73] *La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?*, rapport d'information fait au nom de la délégation aux entreprises du Sénat, 10 juin 2021, op. cit.

Plusieurs experts entendus en audition par le Ceser plaident, dans ce contexte, pour **la création d'emplois de RSSI mutualisés entre plusieurs TPE/PME ou entre plusieurs collectivités.** Les fédérations professionnelles, les têtes de réseaux associatifs, les établissements publics de coopération intercommunale et les départements pourraient jouer un rôle en ce sens, pour aider leurs membres à mieux prévenir les cyberattaques. En Île-de-France, la Fédération du bâtiment d'Île-de-France et la communauté de communes de Puteaux (Hauts-de-Seine) ont, par exemple, chacune créé un poste de RSSI mutualisé pour leurs adhérents. Le CIG Grande couronne (cf. encadré p. 13) structure également un nouveau service en ce sens pour ses collectivités membres. **Le Ceser invite la Région Île-de-France à réfléchir à s'engager dans le soutien (financement, équipement, fonctionnement, etc.) à ce type d'initiatives**, dans le cadre du développement progressif de son action auprès des petites collectivités, des TPME et des petites associations du territoire en matière de sécurité numérique.

2.5 Un enjeu de culture d'entreprise

La mise en œuvre des mesures de protection ne procède pas que de la responsabilité publique : c'est une responsabilité partagée. *« On ne peut pas se protéger uniquement "par le haut" »*[74]. À titre d'illustration : les entreprises du secteur bancaire, outre qu'elles relèvent des organisations surveillées et accompagnées par l'ANSSI, l'ont bien compris en développant des formations proposées à leurs entreprises clientes.

Cette responsabilité est collective y compris dans les entreprises. La majorité des cas de cyberattaques réussies exploite des imprudences ou un défaut de vigilance de la part d'un collaborateur quel qu'il soit. Ainsi, 74 % des entreprises déclarent l'hameçonnage (*phishing*, cf. p. 6) comme vecteur d'entrée principal des attaques qu'elles ont subies[75]. Au-delà des enjeux techniques et des diagnostics de vulnérabilité, **l'utilisateur est le paramètre de sécurité le plus difficile à maîtriser : sensibiliser les collaborateurs, établir une charte informatique, organiser des exercices de manière régulière** pour entretenir la vigilance de chacun sont de nouvelles pratiques à intégrer.

À l'occasion des auditions menées par le Ceser ont été évoquées des difficultés rencontrées avec certains collaborateurs des entreprises, agents des collectivités, salariés ou bénévoles du secteur associatif – voire des manifestations de « rejet » des règles de sécurisation informatique, qui peuvent être vécues comme des contraintes à l'exercice de leur métier, ou des limites à leur liberté. **L'articulation information/formation – sanction est importante :** augmenter la pression sur les collaborateurs lorsqu'un risque extérieur pèse sur l'entreprise (et donc ses emplois) n'est pas forcément synonyme de dégradation des conditions de travail, dès lors que l'entreprise prend ses responsabilités vis-à-vis de ses collaborateurs. Et il faut bien sûr que l'organisation apprenne à gérer « la peur de la faute » tout en distinguant la faute de la malveillance intentionnelle.

Pour l'ANSSI, une bonne approche repose d'abord sur **une analyse partagée des besoins et la construction collective de solutions adaptées.** Les collaborateurs, quel que soit leur statut, sont aussi des ressources : il est utile de les associer en tant que « connaisseurs » des procédures qu'ils utilisent au quotidien. L'objectif n'est pas de faire peser sur les salariés la responsabilité de trouver les solutions, mais de les faire participer à la recherche de solutions. Il est très important que la démarche soit animée au plus haut niveau de l'entreprise : *« le décideur doit prendre connaissance des risques et choisir s'il les accepte ou pas »*[76]. L'ANSSI a développé des ressources pour accompagner les dirigeants d'entreprise à partir de la méthode « EBIOS-Risk Manager[77] » qui repose sur l'élaboration de scenarii associant les *persona* du décideur, du financier, du RSSI, du DSI et des utilisateurs.

[74] Audition de Guillaume CRÉPIN, 16 mai 2023.
[75] *Baromètre annuel de la cybersécurité des entreprises,* CESIN, 30 janvier 2023, op. cit.
[76] Audition de Guillaume CRÉPIN, 16 mai 2023.
[77] La méthode et ses outils d'animation sont disponibles sur le site internet de l'Anssi, consulté le 26 octobre 2023.

Cette approche plaide à la fois pour :

- **La prise en compte de la stratégie de sécurité informatique au niveau de la direction d'entreprise :** elle constitue un des leviers de la stratégie globale d'entreprise ;
- **L'intégration des enjeux de sécurité numérique dans le dialogue social,** ce d'autant que les entreprises adoptent des règlements particuliers ou des chartes destinées à encadrer les pratiques de leurs collaborateurs auxquels peuvent répondre des sanctions disciplinaires ;
- **La mobilisation par l'entreprise du levier de la formation continue des collaborateurs**, en interne ou en externe : les organisations professionnelles, les chambres consulaires, l'ANSSI ou encore CyberMalveillance proposent de nombreux outils. Le service public en ligne « Pix » propose des parcours permettant d'évaluer, développer, et même certifier ses compétences numériques dans cinq domaines dont la protection et la sécurité des données ;
- **La mise à disposition des salariés de matériels et d'espaces de travail numériques sécurisés,** pour que les salariés ne soient pas contraints d'utiliser leur matériel personnel.

À titre d'illustration, la cyberattaque vécue par l'équipe du CIG Grande couronne (cf. encadré p. 13) et ses conséquences ont amené, selon les mots de son directeur général, *« à un changement collectif de culture : la cybersécurité a été intégrée au protocole d'accueil des nouveaux collaborateurs, dans un contexte de turn-over assez fort ; des référents ont été désignés et formés dans les services du CIG ; de nouvelles sécurités sont venues encadrer les pratiques professionnelles (tests, exercices de phishing, etc.). L'intégration du risque psychologique pour les agents, dans le cadre du plan de prévention et de remédiation, participe aussi à ce changement de culture interne. »*

Les bonnes pratiques recommandées aux dirigeants d'entreprises par l'ANSSI

Pour Guillaume CRÉPIN, délégué territorial Île-de-France de l'ANSSI[78], une erreur fréquente est de ne se consacrer qu'aux questions techniques puisque 80 % des attaques relèvent du facteur humain ; **s'en prémunir repose sur le respect de règles d'hygiène numérique simples, qui tiennent en dix points :**

1. Séparer strictement les usages à caractère personnel de ceux à caractère professionnel : les moyens de communication personnels ne doivent pas être utilisés pour des échanges professionnels (courriel, compte d'échange de fichiers / cloud, clé USB etc.) et inversement.
2. Mettre régulièrement à jour ses outils numériques pour garantir leur sécurité.
3. Protéger ses accès par une authentification double-facteur lorsque c'est possible, ou a minima par des mots de passe complexes, sans informations personnelles, uniques et tenus secrets.
4. Ne pas laisser ses équipements sans surveillance lors de ses déplacements.
5. Protéger son espace de travail et l'accès à ses données, en verrouillant son poste de travail (pause, temps du déjeuner, réunion etc.) et en plaçant en lieu sûr le matériel sensible (serveur, support de stockage etc.)
6. Rester vigilant sur Internet et les réseaux sociaux pour préserver son identité numérique et ses données personnelles (exploitées par exemple dans le cadre de « fraude au président »).
7. Protéger sa messagerie professionnelle en portant attention aux messages, liens hypertexte ou pièces-jointes douteuses.
8. Éviter les réseaux non sécurisés pour connecter ses équipements : réseaux wifi publics, bornes de recharge USB publiques, etc. Préférer l'utilisation d'une batterie portable, utiliser un datablocqueur ou bien installer un réseau privé virtuel (RPV).
9. Faire preuve de vigilance lors d'échanges téléphoniques ou en visioconférence : la confidentialité des conversations ne peut pas être assurée sur les réseaux publics.
10. Veiller à la sécurité de son smartphone : éviter notamment de l'emporter pendant des réunions sensibles afin d'éviter le risque d'enregistrement à distance à son insu.

Pour prévenir les attaques, tout commence par une prise de conscience et un questionnement : *« quelles sont les données de valeur de mon entreprise ? où sont-elles stockées ? à qui sont-elles accessibles ? qui pourrait avoir intérêt à récupérer mes données personnelles ou professionnelles ? Ce diagnostic, actualisé régulièrement pour réviser sa stratégie de sécurité informatique, constitue un bon point de départ pour faire l'inventaire de ses besoins et leur faire correspondre des solutions adaptées, sans céder aux sirènes du marketing ».* Le délégué territorial Île-de-France de l'ANSSI invite ainsi les chefs d'entreprise à mobiliser plusieurs leviers d'action :

- **S'appuyer sur une ressource professionnelle formée et disposant des compétences nécessaires :** référent au sein d'une organisation ou d'un syndicat professionnel, des chambres consulaires, RSSI internalisé ou mutualisé entre plusieurs TPE/PME ;
- **Sécuriser les réseaux et équipements professionnels des collaborateurs, compartimenter l'accès aux données et leur stockage :** tous les collaborateurs ont-ils besoin d'avoir accès à toutes les données ?
- **Accompagner et responsabiliser les collaborateurs,** via des exercices de prévention (contre le phishing, les rançongiciels, etc.), des lettres d'information interne et des formations ;
- **Prendre en compte l'écosystème de l'entreprise :** l'ANSSI relève un nombre croissant de pénétration de systèmes d'information exploitant la chaîne logistique des structures qui en sont victimes (prestataires, fournisseurs, sous-traitants, etc.) ;
- **Anticiper : se doter d'un plan de gestion de crise et d'un plan de reprise d'activité,** savoir comment le mettre en œuvre et préparer les collaborateurs pour éviter les mouvements de panique ;
- **Ne pas rester isolé :** faire appel à des prestataires référencés, faire appel aux organisations professionnelles, se tenir informé des évolutions, etc. ;
- **Mobiliser le levier juridique :** clause de sécurisation des données échangées dans les contrats de prestation, charte informatique pour encadrer les pratiques des salariés, etc.

[78] Entendu en audition par la commission Développement économique du Ceser le 16 mai 2023.

2.6 Un enjeu éducatif

L'augmentation des risques numériques invite à **renforcer la formation initiale des Franciliens, en sensibilisant les plus jeunes, dès l'école et à l'université, dans le cadre d'un programme d'éducation à la citoyenneté numérique.** *« On ne peut pas parfaitement réguler internet ou les réseaux sociaux, mais on peut apprendre aux enfants et aux jeunes à exercer leur esprit critique et à développer une autonomie de pensée, pour faire face notamment au risque de désinformation (fake news). La famille et l'École sont bien sûr les premiers cadres de cette éducation*[79]*. »*

L'ANSSI encourage d'ailleurs *« le développement d'une "culture de la sécurité numérique" pour réduire les failles "entre la chaise et le clavier" »*[80]*.*

La certification « Pix », qui a succédé au « B2i »[81] et fait l'objet d'une évaluation obligatoire en fin de cycle 4 au collège et au cycle terminal du lycée, ou le nouvel enseignement de spécialité « Sciences numériques et technologie » dispensé à tous les élèves de seconde des lycées généraux et technologiques, constituent deux des leviers d'action récents de l'Éducation nationale.

CyberMalveillance (voir aussi p. 30) propose un grand nombre d'outils pour sensibiliser le public aux enjeux de la sécurité et de la protection de la vie privée numérique : campagnes de communication, guides et supports d'information, kits pédagogiques, etc. Mais ses moyens sont limités et il s'agit de mobiliser les bons réseaux pour rendre ces ressources accessibles aux jeunes et aux familles.

C'est pourquoi **ces actions mériteraient d'être complétées d'approches complémentaires pour diffuser auprès de tous les jeunes, qui seront demain les collaborateurs des entreprises, collectivités et associations du territoire,** les bonnes pratiques prudentielles élémentaires : sécuriser ses achats en ligne, ses mots de passe, l'utilisation de sa messagerie, la communication sur les réseaux sociaux, etc.

La Région Île-de-France, qui entretient des liens privilégiés avec les académies, les lycées et les universités franciliennes, pourrait ainsi faciliter l'organisation de sessions d'information dans le cadre scolaire avec des acteurs du monde économique. Elle dispose des compétences et moyens d'initier des campagnes de communication et des interventions ciblées sur ces publics, à l'image des campagnes de lutte contre le (cyber)harcèlement qu'elle encourage et finance. Pourquoi ne pas aller plus loin **en embarquant, sur les ordinateurs portables dont la Région équipe les élèves des lycées publics, des vidéos courtes de sensibilisation ?** s'assurer de la diffusion des ressources créées pour ces publics, par exemple celles proposées par CyberMalveillance, via leur environnement numérique de travail (ENT) MonLycée.net ? toucher un plus grand nombre de jeunes en mobilisant les instituts de formation sanitaire et sociale, les résidences universitaires, les missions locales et espaces d'insertion dont elle participe au financement ?

Pour prévenir et lutter contre la menace cyber, des solutions existent. Elles doivent encore arriver à maturité, dans une approche servicielle adaptée à la typologie des acteurs du territoire. Cette démarche, à laquelle la Région prend une part active, est accélérée dans le contexte de l'accueil des Jeux Olympiques et Paralympiques 2024 en Île-de-France. Un effort de coordination apparaît essentiel pour territorialiser ces solutions et les porter à connaissance de tous les acteurs concernés.

[79] Audition du préfet de BOUSQUET, 1er juin 2023.
[80] Audition de Guillaume CRÉPIN, 16 mai 2023.
[81] Brevet Informatique et Internet (B2i) : ancienne certification complémentaire au diplôme national du brevet des collègues, supprimée en 2016 et actualisée par le cadre de référence des compétences numériques, valable de l'école primaire à l'université, élaboré par les ministères chargés de l'Éducation nationale, de la Jeunesse et des Sports et de l'Enseignement supérieur, de la Recherche et de l'Innovation. Il s'organise autour de cinq domaines de compétences numériques qui font désormais l'objet d'une certification délivrée par la plateforme publique Pix.

3 Panorama des solutions proposées aux acteurs économiques franciliens

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.

3.1 La cybersécurité s'inscrit dans une stratégie européenne et nationale

3.1.1 L'Agence nationale de la sécurité des systèmes d'information, autorité de référence au plan national pour les opérateurs vitaux

L'ANSSI a été créée en 2009[82] sous la forme d'un service à compétence nationale. Elle se substitue à la direction centrale de la sécurité des systèmes d'information (DCSSI) du secrétariat général de la défense et de la sécurité nationale (SGDSN), auquel elle reste cependant rattachée. Le SGDSN assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Cette évolution traduit un repositionnement de l'ANSSI et de ses missions, à la fois auprès des administrations centrales et des services de l'État – mais aussi des OIV et des Opérateurs de services essentiels[83] (OSE). La place et les missions de l'ANSSI ont été précisées et complétées par plusieurs lois et règlements afin d'en adapter le périmètre et l'organisation aux évolutions permanentes de la cybermenace :

- L'ANSSI coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information des services de l'État. Elle en élabore les mesures de protection et veille à leur application en menant notamment des audits ou des inspections sur ces systèmes d'information ;
- Bien qu'elle ne dispose pas du statut juridique d'Autorité administrative indépendante (AAI), l'ANSSI, en tant qu'autorité nationale en matière de sécurité et de défense des systèmes d'information, peut imposer aux OIV des mesures de sécurité et des contrôles de leurs systèmes d'information les plus critiques[84] ;
- L'ANSSI contribue à l'orientation de la recherche nationale et européenne en matière de sécurité des systèmes d'information, participe aux négociations internationales sur son périmètre et entretient des relations étroites avec ses homologues étrangers ;
- La loi[85] confère également à l'ANSSI la charge de mettre en œuvre des dispositifs de détection des incidents susceptibles d'affecter la sécurité des systèmes d'information de l'État, des autorités publiques et des OIV publics et privés, de réunir les informations techniques relatives à ces incidents et de proposer l'accompagnement pour y répondre ;
- L'ANSSI délivre des agréments aux dispositifs de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la défense nationale, et assure la formation des agents publics dans le domaine de la sécurité des systèmes d'information ;
- Plus largement, elle se prononce sur la sécurité des dispositifs, produits et services de protection des systèmes d'information relevant de son périmètre (par ex. : dispositifs de création et de vérification de signature électronique) et délivre des habilitations aux prestataires de service.

[82] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé Agence nationale de la sécurité des systèmes d'information, JORF du 8 juillet 2009.
[83] Opérateurs de services essentiels (OSE) : opérateurs tributaires des réseaux ou systèmes d'information, qui fournissent un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société (source : CERT-FR).
[84] Compétence inscrite dans l'art. 22 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF du 19 décembre 2013.
[85] Art. 34 et 35 de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, JORF du 14 juillet 2018.

La sous-direction de la stratégie de l'ANSSI dispose d'une division « sectorielle », qui gère des « portefeuilles » d'opérateurs régulés (transports, assurance, banque, etc.), et d'une division « territoriale » compétente auprès de tous les opérateurs non régulés, qui anime le réseau des délégués territoriaux de l'ANSSI. **Les délégués territoriaux représentent l'ensemble des métiers de l'ANSSI auprès de leurs interlocuteurs. L'ANSSI s'est fixée un objectif-cible de deux délégués par région**, notamment pour accompagner l'élargissement progressif des opérateurs régulés mais aussi répondre aux demandes croissantes des collectivités et des organisations intermédiaires. C'est pourtant peu pour coordonner les réponses aux besoins : **l'agence a besoin de partenaires et relais territoriaux et mise sur l'enrichissement de ses services pour déployer son expertise, en accompagnement d'acteurs intermédiaires, au plus près du territoire.**

La sous-direction des opérations de l'ANSSI réunit des experts chargés de la détection et de la réponse aux cyberattaques relevant du périmètre de l'Agence. **Elle accueille en son sein le CERT- FR (*Computer Emergency Response Team*) qui prend en charge les interventions de premier niveau en cas d'intrusion sur un système d'information d'un organisme public** (ministères, institutions, juridictions, autorités indépendantes, collectivités territoriales, d'un OIV ou d'un OSE, avec une capacité de déploiement rapide et permanente 24h/24 et 7j/7. S'il fournit des informations accessibles à tous (liste des vulnérabilités, état de la menace informatique…) par le biais de son site Internet, **le CERT-FR n'a pas vocation à intervenir directement auprès des particuliers, des TPE et des PME victimes de cyberattaques :** son champ d'action est la sécurisation et la défense des systèmes d'information de l'État, des OVI et des OSE. L'accompagnement de ces publics doit donc être pris en charge par d'autres dispositifs, en particulier CyberMalveillance et des déclinaisons régionales du CERT national en cours de structuration (cf. p. 39).

L'ANSSI édite **une collection de guides en ligne destinés à sensibiliser les entreprises et les administrations aux bonnes pratiques de sécurité numérique** et à les accompagner dans leur mise en œuvre :

- *La cybersécurité pour les TPE/PME en treize questions*, en partenariat avec la direction générale des entreprises, la Confédération des petites et moyennes entreprises (CPME) et FranceNum, octobre 2022 ;
- *Attaques par rançongiciels, tous concernés : comment les anticiper en cas d'incident ?*, en partenariat avec le ministère de la Justice, à partir de retours d'expériences d'établissements publics et de groupes privés, septembre 2020 ;
- Une collection destinée à accompagner les organisations sur l'ensemble des aspects de la gestion de crise cyber : prévention, gestion et communication de crise :
  - *organiser un exercice de gestion de crise cyber* (octobre 2020),
  - *crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique* (décembre 2021),
  - *anticiper et gérer sa communication de crise cyber* (décembre 2021).

L'ANSSI propose **un Cours en ligne ouvert massivement (CLOM) porté par son centre de formation à la sécurité des systèmes d'information, à destination de tous les publics :** SecNumacadémie. Le suivi intégral de ce dispositif, accessible gratuitement, permet la délivrance d'une attestation de réussite.

Dans le cadre du plan France Relance, lancé en septembre 2020 pour relancer l'économie affectée par la crise sanitaire liée à la pandémie de Covid-19, un budget exceptionnel de 136 millions d'euros a été confié à l'ANSSI pour renforcer la sécurité des administrations centrales des ministères, des collectivités territoriales, des établissements de santé et des organismes publics en mobilisant l'écosystème industriel national :

- **Création d'un dispositif de parcours de cybersécurité, permettant aux organismes publics concernés de disposer d'une évaluation de la sécurité de leurs systèmes d'information** et d'un accompagnement par des prestataires sélectionnés par l'ANSSI, de la maîtrise d'ouvrage jusqu'à la mise en œuvre ; fin 2022, le ministre chargé du Numérique a annoncé un élargissement de ces parcours de cybersécurité à de nouveaux bénéficiaires du secteur public, courant 2023 ;

- Lancement d'appels à projets auprès des entreprises de la filière pour **sélectionner des solutions de sécurité accessibles aux plus petites collectivités :** malgré un cofinancement et une référencement clé-en-main pour les collectivités, plusieurs Opérateurs publics de services numériques (OPSN) témoignent[86] de leur difficulté à faire prendre conscience aux maires des petites communes de l'importance de sécuriser l'accès à leurs données ;
- **Cofinancement de centres régionaux de réponse à incident cyber (CSIRT régionaux),** destinés à fournir leur aide aux structures de taille intermédiaire (entreprises, collectivités, associations) en cas d'attaque (cf. p. 39).

Pour accompagner la dématérialisation des démarches administratives en intégrant les enjeux de sécurité, **l'ANSSI a lancé à la toute fin 2022[87] « MonServiceSécurisé », outil qui permet aux administrations et aux collectivités d'évaluer le niveau de sécurité de leur téléservices**, à partir d'un « indice cyber » et d'une liste personnalisée de mesures de sécurité à mettre en œuvre pour leur permettre d'obtenir une homologation.

Un outil de diagnostic, « MonAideCyber », est actuellement en phase de développement pour accompagner les petites structures publiques et privées, incluant les TPE et les associations, à réaliser un premier état de lieux de leur niveau de maturité cyber, prendre connaissance de leurs principales lacunes et identifier des premières actions concrètes et accessibles à mettre en œuvre.

3.1.2 Cybermalveillance : le service public d'information, de prévention et de réaction aux cyberattaques pour le grand public

Le portail cybermalveillance.gouv.fr est animé par le Groupement d'intérêt public (GIP) « Acyma », créé en 2017[88] dans le cadre de la Stratégie nationale pour la sécurité du numérique lancée en 2015 par le Gouvernement[89]. Il a pour mission d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations, de les informer sur les menaces numériques et sur les moyens de s'en protéger – complétant l'action de l'ANSSI hors du périmètre qu'elle encadre directement.

Conçu et incubé par l'ANSSI, le GIP associe l'État (l'ANSSI en tant que service du Premier ministre, les ministères de l'Intérieur, de la Justice, de l'Économie, du Numérique, de l'Éducation nationale et des Armées) et une soixantaine de membres publics et privés parmi lesquels :

- la Commission nationale informatique et libertés (CNIL),
- des agences et opérateurs de l'État : Agence nationale de la cohésion des territoires, Caisse des dépôts, SNCF, Groupe La Poste, Institut national de la consommation,
- des associations d'élus de collectivités territoriales : Régions de France, Association des Maires de France, Association des Petites Villes de France,
- des organisations représentatives des entreprises : Medef, CPME, CCi, U2P, Fevad, etc.
- des associations de consommateurs et d'aide aux victimes : Unaf, UFC-Que Choisir, CLCV, France Victimes, etc.,
- des groupes bancaires et d'assurance : Maif, BNP-Paribas, Caisse centrale de réassurance, France Assureurs, etc.,
- des grandes entreprises éditrices de solutions et d'équipements : Microsoft France, AWS-Amazon, Bouygues Telecom, Orange CyberDéfense, Cisco, Google, Mercatel, etc.

[86] Cybersécurité : les structures mutualisantes peinent à enrôler les maires des petites communes, *La Gazette des Communes*, publié le 6 octobre 2023.
[87] Communiqué de presse du 13 décembre 2022 : « MonServiceSécurisé : l'ANSSI lance une nouvelle solution pour sécuriser et homologuer les services publics en ligne ».
[88] Arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance, JORF du 5 mars 2017
[89] La Stratégie nationale pour la sécurité du numérique, annoncée par le Premier ministre en juin 2015, peut être consultée en version intégrale sur le site internet de l'Anssi.

Le premier métier du GIP est de porter assistance aux particuliers, aux entreprises et aux administrations victimes d'actes de cybermalveillance sous la forme **d'un « guichet unique » permettant à la fois l'accompagnement aux démarches administratives pour le dépôt de plainte et la mise en relation avec des prestataires référencés**[90] capables de prendre en charge la reprise d'activité des équipements et réseaux informatiques infectés.

Cette mission est complétée, depuis 2022, par la mise en place **d'un service réservé aux professionnels (entreprises, collectivités et associations) qui souhaitent organiser un diagnostic préventif de sécurité sur leurs équipements**, accompagné par un professionnel en sécurisation des systèmes d'information labellisé « ExpertCyber » (label créé avec le soutien de l'AFNOR, voir aussi p. 21). Ce faisant, CyberMalveillance contribue à aider ces publics à se repérer dans la multiplicité des offres commerciales proposées par les prestataires en sécurité informatique.

Pour sensibiliser le grand public, CyberMalveillance met à disposition des supports d'information (vidéos, fiches, kit de sensibilisation, affiches, stickers, mémos, etc.) pour comprendre les cybermenaces et savoir comment y réagir, ainsi que des bonnes pratiques à adopter pour assurer sa sécurité numérique : installer un antivirus, faire les mises à jour de ses appareils et logiciels, gérer ses mots de passe, mettre en place des sauvegardes, sécuriser son site Internet, adopter des bonnes pratiques sur les réseaux sociaux, la sécurité au télétravail et sur les réseaux publics wifi, etc. **Des fiches-mémo synthétiques au format « affiche » peuvent être téléchargées pour diffuser ces conseils dans les locaux des administrations, des entreprises et des associations.** Ces supports sont complétés par une collection de guides adressés à des publics spécifiques :

- *Guide de cybersécurité à destination des dirigeants de TPE, PME et ETI* (publié en mai 2021) ;
- *Les obligations et responsabilités des collectivités locales en matière de cybersécurité* (publié en juillet 2022), complété par une *Méthode clé en main pour sensibiliser les agents des collectivités* (publiée en novembre 2022) et un programme de sensibilisation des élus locaux ;
- SensCyber, programme de sensibilisation à la cybersécurité en ligne lancé en juin 2023, destiné à tous les agents de la fonction publique, développé notamment avec le Centre national de la fonction publique territoriale (CNFPT) ;
- *Cyber Guide Famille* (publié en octobre 2023).

CyberMalveillance coanime, avec l'ANSSI, le Mois européen de la cybersécurité, initiative conçue par l'Agence de l'Union européenne pour la cybersécurité (ENISA, voir aussi p. 17). Chaque année en octobre, CyberMalveillance invite les acteurs publics, privés et associatifs concernés à se mobiliser pour proposer un programme de sensibilisation pédagogique à destination de tous les publics. L'édition 2023 de ce « Cybermoi/s », officiellement lancée au Campus Cyber (cf. p. 22), a eu pour thème la fraude par ingénierie sociale, en pleine expansion (cf. p. 7). La Région Île-de-France a relayé l'opération auprès de ses agents.

À cette occasion, **CyberMalveillance a invité 83 organisations, parmi lesquelles la Région Île-de-France[91] et de nombreuses organisations et fédérations professionnelles (CPME, MEDEF, U2P par exemple), à signer une *CharteCyber*** (cf. annexe en p. 52) par laquelle elles s'engagent à *« démontrer l'importance de la cybersécurité au sein de leur entité au travers du respect de ces engagements, en témoigner auprès de leur écosystème et encourager toutes les autres organisations à adopter cette démarche ».*

3.1.3 L'Observatoire de la sécurité des moyens de paiement

Dans le cadre de ses missions de régulation du secteur bancaire, la Banque de France (cf. encadré p. 8) assure le secrétariat permanent de l'Observatoire de la sécurité des moyens de paiement (OSMP), chargé de promouvoir le dialogue et les échanges d'informations entre les acteurs intéressés par la sécurité et le bon fonctionnement des moyens de paiement scripturaux.

[90] Descriptif de la méthode de référencement et liste de prestataires sur le site internet de CyberMalveillance, consulté le 26 octobre 2023.
[91] Source : site internet de CyberMalveillance, consulté le 26 octobre 2023.

Il réunit, aux côtés de la puissance publique (dont les forces de police/gendarmerie et de justice, la CNIL et la direction générale de la concurrence, de la consommation et de la répression des fraudes-DGCCRF) et de parlementaires, les « offreurs » du marché des paiements (constructeurs de matériels, éditeurs de solutions logicielles) et leurs utilisateurs (représentant des commerçants, des entreprises et des consommateurs), sous la présidence du gouverneur de la Banque de France.

Il a pour mission de suivre les mesures de sécurité adoptées par les acteurs du marché des paiements et leurs clients, d'établir des statistiques agrégées de fraude et de proposer des recommandations pour les maitriser. Pour faire face à des fraudes qui relèvent de plus en plus de l'ingénierie sociale, **l'OMSP plaide pour une évolution du droit pour améliorer la protection des consommateurs, des entreprises et des professionnels et à plus de transparence entre les acteurs de la chaine des paiements** (vendeur, consommateur et prestataire de services de paiement)[92].

Pour l'OMSP, la prévention de la lutte contre la fraude aux moyens de paiement scripturaux nécessite d'agir simultanément et en cohérence sur quatre leviers :

- **La mise en place de techniques d'authentification forte du payeur** par les opérateurs bancaires et les prestataires de traitement des flux de paiement ;
- **L'identification des opérations « à risque » à tous les maillons de la chaine de paiement :** en entreprise, cela peut passer par la systématisation du « contre-appel » vers un numéro déjà référencé pour vérifier l'identité d'un donneur d'ordre ou d'un fournisseur ;
- **Le renforcement de la sécurité physique et logique des systèmes d'information et de gestion des transactions :** par exemple en distinguant la base « fournisseurs » de la base « salariés », en chiffrant l'accès aux bases de données, en segmentant l'accès des collaborateurs de l'entreprise aux données, etc. ;
- **La vigilance des utilisateurs,** qui a tendance à s'affaiblir avec le temps et demande donc des « rappels » : exercice interne de perméabilité, formations internes, tests, etc.

L'OMSP soutient aussi le développement de nouveaux outils de prévention de la fraude : à titre *d'exemple*, un dialogue est engagé avec les opérateurs de téléphonie pour éviter l'usurpation, par des réseaux de fraudeurs, des numéros d'appel des établissements bancaires[93].

3.1.4 Cyberscore et filtre anti-hameçonnage « grand public » : deux nouveaux dispositifs nationaux en cours de déploiement

Sur une initiative parlementaire, la loi[94] a créé **un « Cyberscore » afin que les internautes puissent connaître le niveau de sécurisation de leurs données sur les grandes plateformes numériques, les messageries instantanées et les sites de visioconférence qu'ils utilisent**. Les parlementaires ont prévu qu'un audit soit effectué par des prestataires qualifiés par l'ANSSI, *« présenté au consommateur de façon lisible, claire et compréhensible et est accompagné d'une présentation ou d'une expression complémentaire, au moyen d'un système d'information coloriel[95] »* – à l'image du « Nutriscore » pour les produits alimentaires. Le dispositif est entré en application le 1er octobre 2023, pourtant son cahier des charges n'est pas encore très clair et reste dans l'attente d'un arrêté destiné à fixer les critères pris en compte par l'audit, la validité du « score » et ses modalités de présentation.

[92] Communiqué de presse du 16 mai 2023 **:** *« L'Observatoire de la sécurité des moyens de paiement émet des recommandations sur le remboursement des victimes de fraude » **;*** **liste des recommandations dans** le rapport publié à la même date**, disponible sur le site internet de la Banque de France, consulté le 26 octobre 2023.**
[93] Audition de Julien LASALLE, 1er juin 2023.
[94] Loi n°2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public, JORF du 4 mars 2022.
[95] Art. L111-7-3 du code de la consommation.

Par ailleurs, le ministre en charge du Numérique a présenté en Conseil des ministres du 10 mai 2023 un Projet de loi (PJL) visant à *« sécuriser et réguler l'espace numérique »*, destiné, selon son exposé des motifs[96], à *« restaurer la confiance nécessaire au succès de la transition numérique »,*

Le PJL vise notamment à traduire, dans la législation française, les nouvelles directives européennes dans le champ du numérique[97] adoptées à l'occasion de la dernière présidence française de l'Union européenne. Le texte comporte une série de mesures et dispositions destinées à protéger les particuliers (en particulier l'accès des mineurs aux sites proposant des contenus à caractère pornographique, et un renforcement des sanctions des personnes condamnées pour haine en ligne ou cyberharcèlement), les entreprises et les collectivités (en réduisant leur dépendance aux grands acteurs du marché du numérique). Pour lutter contre les tentatives de déstabilisation et de désinformation, le PJL prévoit d'étendre aux plateformes en ligne l'interdiction de diffusion de médias étrangers faisant l'objet de sanctions internationales.

L'article 6 du PJL met en place **un « filtre de cybersécurité anti-arnaque » grand public,** qui vise à protéger les particuliers contre les tentatives d'hameçonnage, d'arnaques financières (paiements frauduleux notamment), d'usurpation d'identité et d'utilisation de données personnelles à des fins malveillantes.

Concrètement :

- Les internautes, dans leur quotidien ou au travail, verront s'afficher un message d'avertissement lorsqu'ils voudront accéder à une adresse internet pour laquelle il existe un risque avéré d'arnaque ou d'escroquerie (par exemple à la suite de la réception d'un mail ou d'un SMS frauduleux) ;
- Les sites « cybermalveillants » seront identifiés par des agents habilités de l'autorité administrative sous le contrôle d'une personnalité qualifiée indépendante rattachée à la Commission nationale de l'informatique et des libertés (CNIL) ;
- Si les faits persistent au-delà d'une période de sept jours, ou si l'éditeur du service associé à l'adresse internet n'est pas identifiable, l'autorité administrative pourra demander aux fournisseurs d'accès à internet, aux fournisseurs de systèmes de résolution de noms de domaine et aux fournisseurs de navigateur internet de prendre toute mesure destinée à empêcher l'accès au site.

Adopté en première lecture par le Sénat le 5 juillet puis par l'Assemblée nationale le 17 octobre, le texte est en attente de la convocation d'une commission mixte paritaire annoncée en décembre 2023, au moment où ce rapport est rédigé.

[96] Le texte du projet de loi et l'intégralité du dossier législatif sont disponibles sur le site du Sénat, consulté le 27 octobre 2023.

[97] Dans son avis sur le projet de loi rendu le 27 avril 2023, le Conseil d'État note en effet que le projet de loi s'inscrit dans le projet de constitution d'un « marché unique du numérique européen » en prévoyant les mesures nécessaires à l'adaptation du droit national et à la mise en œuvre de trois règlements européens :

- le règlement (UE) n° 2022/1925 du 14 septembre 2022, JOUE du 14 septembre 2022, sur les services et marchés numériques (*Digital Markets Act* – DMA) entré progressivement en application depuis le 2 mai 2023 : Il prévoit notamment que les contrôleurs d'accès ne peuvent plus imposer les logiciels les plus importants (comme les navigateurs ou les moteurs de recherche par exemple) par défaut à l'installation de leur système d'exploitation. Ils ne pourront plus non plus réutiliser les données personnelles d'un utilisateur à des fins de publicité ciblée, sans son consentement explicite. Parmi les premières entreprises concernées désignées par la Commission Européenne : Alphabet (Google), Amazon, Apple, Meta (Facebook, Instagram), Microsoft et ByteDance (TikTok).
- le règlement (UE) 2022/2065 du 19 octobre 2022, JOUE du 27 octobre 2022, relatif à un marché unique des services numériques (*Digital Services Act* – DSA) qui entrera en application le 17 février 2024 : il cherche à limiter la diffusion de contenus illicites (incitations à la haine ou à la violence, harcèlement, pédopornographie, apologie du terrorisme…) et la vente de produits illicites en ligne. Les plateformes (fournisseurs d'accès à internet, services en nuage ou *cloud*, places de marché, réseaux sociaux, etc.) ont l'obligation de coopérer avec des *« signaleurs de confiance » :* organismes et associations labellisés en vertu de leur expertise et qui verront leurs notifications traitées en priorité.
- le règlement (UE) 2022/868 du 30 mai 2022, JOUE du 3 juin 2022, portant sur la gouvernance européenne des données (*Data Governance Act* – DGA) qui entrera en application le 24 septembre 2023.

3.2 Les acteurs-clés de la prévention et de la gestion des incidents de sécurité numérique en Île-de-France

3.2.1 Le consortium régional Cybiah au sein du Campus Cyber de La Défense

Le projet Cybiah s'inscrit dans le réseau des pôles européens d'innovation numérique (EDIH pour *European Digital Innovation Hub),* issus du programme pour une Europe numérique (*DIGITAL Europe*). L'objectif des EDIH est de structurer une présence régionale qui offre aux acteurs locaux toutes les opportunités d'un réseau européen : il s'agit de **fournir un accompagnement et des services à des entreprises locales, dans la même langue et tenant compte de la culture d'innovation locale.** Les 150 EDIH sont récents, issus de deux vagues de labellisation par la Commission européenne fin 2022 et au printemps 2023. Les seize EDIH français sont en phase de structuration de leur offre de services et des modalités dans lesquelles ils adresseront leurs publics potentiels.

Le projet francilien, baptisé Cybiah (pour *CYBersecurity and AI Hub*), compte douze membres parmi lesquels l'école d'ingénieurs EPITA, la Métropole du Grand Paris, la CCI Paris-Île-de-France, l'Institut national de recherche en informatique et automatique (INIRIA) et l'EPT Paris-Ouest-La Défense, aux côtés d'entreprises et de start-ups (FiGroup, Aleia, Sekoia, Erium), la communauté de « *hackeurs* éthiques » de *Yes we hack* et l'association Hub France IA. Il est hébergé et coordonné par le Campus Cyber (cf. p. 22).

Le modèle des EDIH repose sur un financement en synergie : 50 % des fonds sont apportés par le programme *DIGITAL Europe* et l'autre partie repose sur des cofinancements. Cybiah bénéficie ainsi de 6 millions d'euros de financements dont 3 millions d'euros par la Commission européenne, 2 millions d'euros du Fonds européen de développement régional (FEDER) via la Région Île-de-France qui en est l'autorité de gestion et 1 million d'euros de chiffres d'affaires en cible. L'objectif est de terminer le projet à l'équilibre (pas de bénéfice partagé entre les membres).

La Région Île-de-France, deuxième contributeur financier du dispositif, a choisi de flécher sa participation sur les seules PME. Les TPE pourront faire appel aux services de l'EDIH mais il leur faudra trouver d'autres sources de financement ; et les collectivités devront s'acquitter d'un reste à charge plus important que les PME pour s'acquitter du prix des prestations d'accompagnement facturées par le programme, puisqu'elles ne pourront pas bénéficier de la part FEDER. Pourtant, le versement des fonds européens du programme *DIGITAL* est conditionné à des objectifs de résultats qui incluent les entreprises et les collectivités locales[98]. **Cette lecture désalignée des objectifs du programme par ses deux principaux contributeurs financiers est source de complexité : une simplification serait bienvenue alors que le défi de la sécurité numérique est bien un enjeu collectif.**

Cybiah propose **une démarche intégrée basée sur le tryptique *« sensibiliser pour orienter et accompagner »,*** qui repose sur le lien de confiance entre le dirigeant de l'entreprise et un expert mandaté par l'EDIH pour le conseiller de la phase d'évaluation à l'implémentation d'une solution de cybersécurité adaptée.

Le « parcours EDIH » s'organise en plusieurs étapes successives :

1. L'entrée dans le parcours d'accompagnement : PME et collectivités locales, orientées via le site internet de l'EDIH, un relais d'information ou par prospection via leurs fédérations professionnelles par exemple, sont soumises à une évaluation de leur maturité cyber. **La Région pourrait d'ailleurs aider Cybiah à cibler plus efficacement, parmi les 800 000 PME du territoire, celles qui en auraient le plus besoin, à partir de sa connaissance du tissu économique francilien.** Cette mise en relation constituerait une façon de prolonger la décision politique d'accompagner les entreprises, particulièrement manifeste pendant la crise du Covid-19, en les aidant à prévenir de nouveaux risques : **c'est aussi une manière d'améliorer le « retour sur investissement » de l'argent public versé aux entreprises par la Région.**

[98] Audition d'Anne-Sophie COLLÉAUX, 30 juin 2023.

2. Au besoin, l'expert cyber de Cybiah propose ensuite un diagnostic de cybersécurité « réel » (c'est-à-dire intrusif sur le système d'information et pas seulement basé sur du déclaratif du dirigeant). Ce diagnostic, personnalisé, prend en compte le secteur d'activité de l'entreprise, ses ressources, les enjeux de gouvernance, le facteur humain etc. Ainsi, selon son degré de maturité cyber, chaque structure est orientée vers des dispositifs de droit commun (par ex. MonAideCyber en cours de développement par l'ANSSI, cf. p. 30) ou peut bénéficier d'un diagnostic plus étoffé de cinq à dix jours.
3. Il en ressort un plan de sécurisation qui articule de la formation, des recommandations et des solutions en *test before invest*, appliquées au système d'information ou à un processus métier de l'entreprise. L'objectif étant que l'entreprise constate par elle-même les bénéfices d'investir dans la cybersécurité, par la preuve de concept. Dans le respect des règles de la libre concurrence, la commercialisation d'une offre complète se fait ensuite sur le marché, à partir des recommandations émises dans le cadre de l'accompagnement Cybiah.
4. Afin d'assurer un continuum de sécurité, le référentiel de diagnostic sera commun à la direction générale des entreprises, BpiFrance, l'ANSSI et Cybiah. Ainsi, une PME « sortante » du parcours guidé Cybiah pourra se voir accompagner vers un nouveau dispositif d'accompagnement financier (par exemple le « Chèque Cyber » proposé par la Région Île-de-France, cf. p. 36 et 53) afin d'assurer sa transition progressive vers un niveau supplémentaire de maturité cyber.

À terme, l'enjeu est d'identifier les bons leviers pour passer à l'échelle, en déployant la méthode en relais et en synergie avec les services déconcentrés de l'État, régions, départements, syndicats mixtes, campus territoriaux cyber, réseaux d'entreprises, chambres consulaires, syndicats et fédérations professionnelles, etc.

Le lancement opérationnel de Cybiah est prévu fin 2023. Une équipe est en cours de recrutement, avec une cible à trois ans de sept à huit collaborateurs en fin de projet.

3.2.2 L'accompagnement financier des acteurs économiques par la Région

En visite le 16 mars 2023 au Campus Cyber, la présidente de Région a annoncé trois mesures destinées à accompagner les entreprises franciliennes face au développement des cyberattaques, présentant la sécurité informatique comme *« un enjeu majeur de protection du patrimoine des entreprises, de compétitivité et de création de valeur »*[99] *:* outre le soutien au programme Cybiah, et le lancement d'un CSIRT régional (cf. p. 39), **un *« pack cybersécurité »* composé de deux nouvelles aides régionales qui « *incarnent le volet préventif de la politique cyber mise en œuvre par la Région »*** en faveur des entreprises franciliennes. Ces nouveaux dispositifs étaient esquissés dans le SRDEII 2022-2028[100].

Le Conseil régional a voté de nouveaux crédits pour concrétiser ces projets dans le cadre du Budget supplémentaire 2023[101], traduits dans un nouveau dispositif « Chèques cyber » composé de deux aides :

- **Un chèque « Diagnostic Cyber » d'un montant maximum de 5 000 euros** destiné à financer la réalisation de diagnostics et la formalisation de plans d'actions associés ;
- **Un chèque « Investissement Cyber » d'un montant maximum de 10 000 euros,** conditionné à la réalisation d'un diagnostic de cybersécurité et destiné à soutenir les dépenses d'équipement.

[99] La Région parie sur la cybersécurité, *Le journal du Grand Paris,* 16 mars 2023
[100] Délibération du Conseil régional n° CR 2022-029 adoptée le 19 mai 2022, op. cit.
[101] Délibération du Conseil régional n° CR 2023-018 adoptée le 31 mai 2023.

Trois millions d'euros sont fléchés sur ce dispositif, dont deux millions en autorisation de programme et un million en autorisation d'engagement.

Le dispositif fonctionne sur la base d'un cofinancement (pourcentage d'intervention final de la Région calculé sur la base du total des dépenses éligibles justifiées par facture, avec un minimum déclenchant l'éligibilité et un montant de subvention maximum pour chacune des deux aides).

La délibération de la commission permanente associe la CCI Paris Île-de-France à la gestion de ces deux nouvelles aides, au regard de l'art. L1611-7 I du code général des collectivités territoriales qui prévoit que *« les collectivités territoriales et leurs établissements publics peuvent confier à un tiers l'instruction des demandes et la préparation des décisions d'attribution des aides et prestations financières qu'ils assument ou instituent. ».*

Les deux aides sont cumulables mais, pour percevoir le chèque « Investissement Cyber », il faudra prouver que l'entreprise a effectué un audit par un expert labellisé (mêmes labels que ceux du chèque « Diagnostic ») : cet élément du règlement d'intervention, qui pourrait apparaître restrictif au premier abord, **répond aux difficultés exprimées par les entreprises d'une offre de services encore confuse** (cf. point. 2.3, p. 20) en les amenant à retenir des solutions d'équipement sur la base d'un diagnostic conduit par un professionnel sourcé.

Pour le chèque « Diagnostic Cyber », le choix du prestataire, qui appartient à l'entreprise dans le respect du droit de la concurrence, est soumis à deux conditions cumulatives :

- L'entreprise prestataire devra être *« labellisée par un acteur reconnu »* ; les labels reconnus par le règlement d'intervention sont ceux de l'ANSSI, le label « France Cybersécurité » des industriels de la cyber protection et un « label CCI » (en cours d'élaboration) ;
- Elle doit avoir son siège ou son établissement situé en Île-de-France : **cette disposition paraît intéressante pour renforcer l'écosystème local cyber,** un enjeu soulevé par plusieurs des experts entendus par le Ceser dont l'ANSSI et Cybiah, et qui correspond aux orientations exprimées par les TPME en faveur « d'achats locaux » selon FranceNum[102] (cf. p. 21).

À l'occasion du salon Vivatech en juin, la présidente de Région a indiqué que ces aides seraient finalement réservées *« aux PME de plus de 10 salariés »*[103]*,* ce que confirme le règlement d'intervention[104] adopté par la commission permanente du Conseil régional le 21 septembre 2023. L'Exécutif régional[105] indique cibler ces aides sur cette catégorie d'entreprises[106] (incluant les associations de plus de 10 salariés ayant une activité économique lucrative) compte tenu de son exposition croissante au risque numérique ; par ailleurs, l'aide de la Région veut s'inscrire en complémentarité des actions engagées par l'État et sans « doublonnement » – les TPE et petites associations étant adressées par CyberMalveillance.

Le Ceser regrette cette approche laquelle amène à exclure de ce dispositif les TPE qui représentent 78,5 % des entreprises franciliennes[107] ainsi qu'un grand nombre d'associations, alors que ces deux catégories n'échappent plus au risque de cyberattaque.

[102] *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023*, FranceNum / Crédoc, op. cit.
[103] *À Viva Technology, du nouveau pour que l'Île-de-France reste la 1ère Smart Région d'Europe*, actualité publiée sur le site internet de la Région le 15 juin 2023, consultée le 27 octobre 2023.
[104] Délibération de la commission permanente du Conseil régional n° CP 2023-327 adoptée le 21 septembre 2023.
[105] Audition d'Alexandra DUBLANCHE, vice-présidente du Conseil régional d'Île-de-France chargée de la relance, de l'attractivité, du développement économique et de l'innovation, entendue en audition par la commission Développement économique du Ceser Île-de-France le 19 octobre 2023.
[106] Plus précisément, sont éligibles les PME comptant entre 10 et 249 salariés et dont le chiffre d'affaires n'excède pas 50 millions d'euros ou dont le total bilan n'excède pas 43 millions d'euros, dont le siège et/ou l'établissement est situé en Île-de-France, immatriculées depuis au moins six mois au Registre du commerce et des sociétés et/ou au Répertoire des métiers et qui ne répondent pas à la notion « d'entreprises en difficulté ». Source : portail internet des aides de la Région, consulté le 27 octobre 2023.
[107] D'après les *Chiffres-clés de la région Île-de-France 2023*, Institut Paris Région avec l'Insee et la Cci Paris Île-de-France, juin 2023.

Parce ces deux nouvelles aides répondent à un vrai besoin, le Ceser propose de **fondre le Chèque Cyber et le Chèque numérique[108] en une nouvelle aide unique :**

- **Associant accompagnement à la transition et à la sécurisation numérique,** qui ne peuvent pas être envisagées séparément ;
- **Accessible à une plus grande diversité** de catégories de structures éligibles (incluant les entreprises de service par exemple) ;
- **Dans une approche élargie du type de dépenses éligibles à l'aide régionale.** La plupart des solutions numériques fonctionnent sur le régime de la licence, qui n'est pas considérée comme une dépense éligible à une subvention d'investissement ; or, la sécurité informatique et numérique ne peut pas se contenter d'une intervention unique : c'est un enjeu d'actualisation permanente, dans la durée. La nouvelle aide unifiée pourrait aussi prendre en compte les dépenses d'assistance à maîtrise d'ouvrage pour l'implémentation de solutions sur la base des résultats du diagnostic de sécurité numérique.

[108] Délibération de la commission permanente du Conseil régional n° CP 2023-246 adoptée le 5 juillet 2023, qui modifie le règlement d'intervention relatif aux *« Chèques en faveur de la transition numérique et écologique des artisans et commerçants franciliens ».*

Focus : La trajectoire cybersécurité de la collectivité régionale[109]

Au cours de ces dernières années, la Région Île-de-France a posé les bases de sa transformation numérique : installation du nouveau siège de la Région à Saint-Ouen-sur-Seine, dématérialisation d'un nombre croissant de processus, mise en place du télétravail et du *flex-office*, création d'« Île-de-France Smart Services » sans oublier le développement du très-haut-débit sur tout le territoire, l'équipement en wifi et la remise d'ordinateurs portables aux élèves et de tablettes aux agents des lycées.

Dans la continuité de cet effort, un Pôle Transformation numérique (PTNum) a été créé au 1er janvier 2022 au sein des services de la Région, pour structurer cette politique en réunissant des acteurs auparavant répartis dans différents services régionaux. Le PTNum regroupe trois directions :

- La direction des systèmes d'information, qui a la responsabilité des infrastructures, de la bureautique et la gestion des systèmes d'information des services « métiers » de la Région ;
- La direction du numérique et de l'innovation, qui structure le pilotage des grands projets d'innovation, accompagne la transformation numérique des lycées et comprend la mission « grands projets numériques » qui vise à améliorer la qualité de service aux usagers par le développement de plateformes numériques de services ;
- La direction de la donnée, chargée de développer la gouvernance de la donnée, en interne et en lien avec les partenaires de la Région : qualité et cohérence de la donnée et de ses usages, conformité réglementaire (RGPD notamment), accessibilité des données régionales pour les usagers, expérimentation du recours à l'intelligence artificielle dans le pilotage des dispositifs régionaux.

En matière de cybersécurité, l'accueil de grands évènement sportifs internationaux en Région Île-de-France a constitué une opportunité d'accélérer le déploiement des mesures inscrites dans la feuille de route, compte tenu du haut niveau d'exposition au risque cyber qu'accompagne l'organisation de ces rassemblements (cf. p. 6). La Région Île-de-France est l'un des trois acteurs principaux de l'organisation des Jeux Olympiques et Paralympiques 2024 avec le COJO et la Ville de Paris, ce qui crée une tension favorable à la mobilisation collective et offre un horizon temporel de réalisation pour la stratégie de cybersécurité portée par le PTNum.

L'objectif est d'atteindre en 2024 un niveau de maturité conforme aux recommandations de l'ANSSI :
- une gouvernance SSI mature et éprouvée,
- une organisation résiliente capable de réagir en cas de crises de cybersécurité,
- des agents sensibilisés aux enjeux et bonnes pratiques en matière de cybersécurité,
- des outils opérationnels pour détecter les incidents de sécurité et y répondre, dans un environnement technologique conforme à l'état de l'art de la filière SSI.

Le PTNum a piloté, avec le service des ressources humaines de la Région, la mise à jour de la « Charte des usages numériques, informatiques et de données » à destination des agents du siège. La charte révisée tient compte de l'évolution des pratiques informatiques et numériques, dans un contexte de développement du télétravail, et des obligations faites à la Région et à ses agents par l'application du RGPD. La même démarche est conduite vis-à-vis des agents de la Région dans les lycées, avec l'écriture d'une PSSI spécifique commune aux trois académies concernées (Paris, Créteil et Versailles) et à la Région.

Ces démarches sont complétées par des actions d'information et de sensibilisation des agents dans le cadre du Cybermoi/s, des tests pour évaluer leur niveau de maturité en cybersécurité et le développement de formations CLOM à partir de cadres d'usage métiers concrets.

[109] Audition de Bernard GIRY, le 5 septembre 2023.

3.2.3 UrgenceCyber Île-de-France, la « cybercaserne » régionale

Les CSIRT *(Computer Security Incident Response Team)* sont des centres de réponse régionalisés aux incidents cyber qui visent des organisations de taille intermédiaire du territoire. Leur émergence participe de la stratégie de l'ANSSI pour étendre la réponse aux incidents cyber à ces organisations, en permettant de fournir localement un service de premier niveau gratuit, complémentaire des services du CERT-FR (cf. p. 29) et de la plateforme CyberMalveillance (cf. p. 30). Ils ont vocation à traiter les demandes d'assistance et à mettre en relation ces organisations avec des prestataires de réponse à incident. Leurs équipes portent également des missions de prévention, de sensibilisation et d'accompagnement dans la montée en compétence des acteurs de leurs territoires.

Ils bénéficient d'un financement dans le cadre du plan France Relance, ainsi que d'un accompagnement méthodologique sous la forme d'un parcours d'incubation assuré par l'ANSSI pendant trois ans pour former les agents de ces entités. L'ensemble des Régions métropolitaines est entré dans le programme, hormis la Région Auvergne-Rhône-Alpes. Sur les douze CSIRT régionaux prévus, neuf[110] étaient opérationnels à la rentrée 2023.

Annoncée par la présidente de Région comme *« la cybercaserne »* régionale, la déclinaison francilienne du dispositif est encadrée par une convention[111] de partenariat signée entre l'ANSSI et la Région au printemps 2022. Le projet est chiffré à 2,6 millions d'euros dont 1 million versé par l'ANSSI[112]. **Pour l'Exécutif régional, le CSIRT « *complète ainsi l'offre cyber aux PME, prenant en charge le volet défensif* *lorsque les entreprises sont victimes d'attaques cyber »*[113].** Sa mise en œuvre répond aussi à l'intérêt de la Région, en contribuant à améliorer le niveau de protection des entreprises dont elle est un partenaire important, selon la doctrine *« zero-trust »*[114].

Baptisé « UrgenceCyber Île-de-France », le CSIRT francilien s'adressera aux PME, aux ETI, aux collectivités territoriales et établissements publics associés de taille moyenne (définies comme comptant plus de 5 000 habitants) **et aux associations du territoire**[115]. Les autres catégories de bénéficiaires, dont les TPE et les petites collectivités ou établissements publics, sont invités à se rapprocher directement de CyberMalveillance qui, malheureusement, n'a pas de présence territoriale.

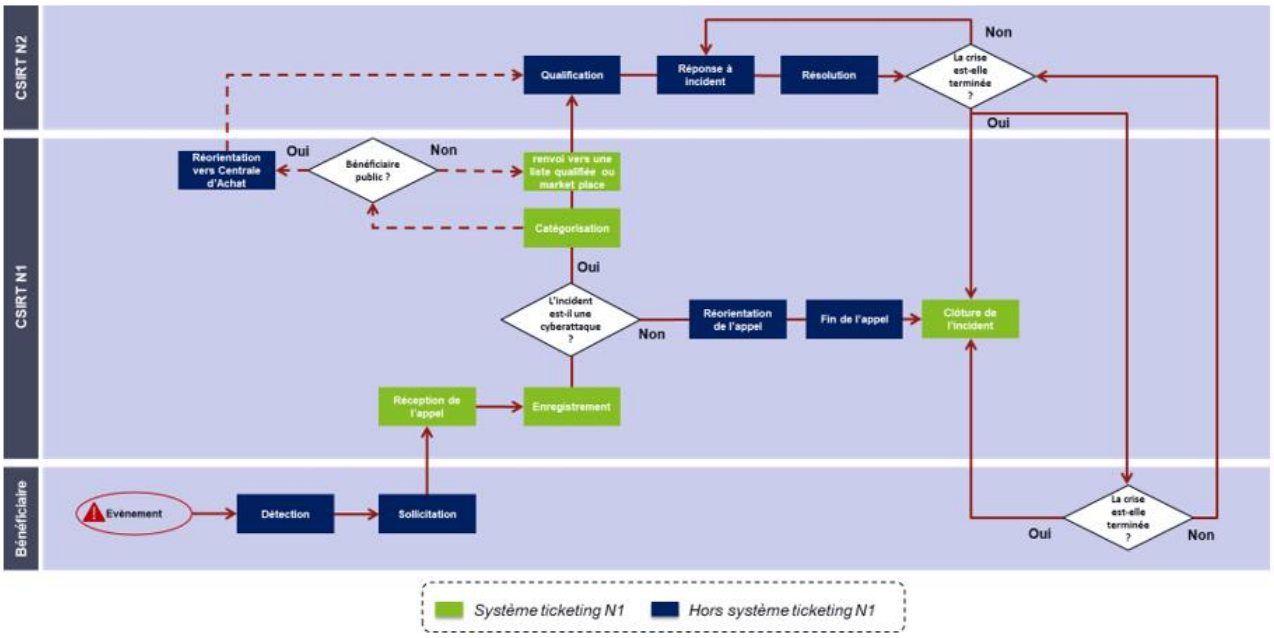
Concrètement, UrgenceCyber Île-de-France consiste en **un centre d'assistance accessible via une plateforme d'appels téléphoniques :**

- Des experts évalueront d'abord l'incident, analyseront l'attaque et ses dégâts et proposent un accompagnement juridique aux victimes de cyberattaques (niveau 1) ;
- L'organisme visé sera ensuite orienté vers des partenaires agréés spécialisés en investigation et traitement des incidents de cybersécurité (niveau 2) ; ces prestataires sont en cours de référencement via un appel à manifestation d'intérêt (voir en p. 22).

La Région Île-de-France a fait le choix de recourir à un marché public pour donner corps à ce projet (d'autres collectivités régionales ont fait le choix d'un GIP ou d'une forme juridique associative). Un appel d'offres a été publié en février 2023. Un marché public a été publié le 3 février et attribué le 7 juillet 2023[116]. **Le lancement public de la plateforme est annoncé avant la fin de l'année 2023.**

---

[110] Bourgogne-Franche-Comté, Centre-Val de Loire, Grand-Est, Hauts-de-France, Normandie, Nouvelle-Aquitaine, Occitanie, Pays de la Loire, Provence-Alpes-Côte-d'Azur, d'après le site internet du CERT-FR, consulté le 27 octobre 2023.
[111] Convention approuvée par délibération de la commission permanente du Conseil régional n° CP 2022-123 du 23 mars 2022.
[112] Délibération de la commission permanente du Conseil régional n° CP 2022-483 du 19 novembre 2022.
[113] D'après l'exposé des motifs de la délibération de la commission permanente du Conseil régional n° CP 2023-327 adoptée le 21 septembre 2023, op. cit.
[114] Audition de Bernard GIRY, 5 septembre 2023.
[115] D'après l'appel à manifestation d'intérêt pour le référencement de prestataires cybersécurité (niveau 2) franciliens par le CSIRT Île-de-France, publié sur le site internet de la Région, consulté le 26 octobre 2023 (voir aussi p. 22).
[116] Avis d'attribution de marché public n° 23-94497 : Prestations de déploiement du CSIRT de la Région Île-de-France - Lots 1 à 3, BOAMP du 7 juillet 2023.



Description du « parcours usager » du CSIRT régional, publiée dans le cadre de l'appel à manifestation d'intérêt pour le référencement de prestataires cybersécurité (niveau 2) franciliens par le CSIRT Île-de-France, op. cit.

Les services gratuits fournis par la cybercaserne régionale

La convention de partenariat signée entre l'ANSSI et la Région Île-de-France engage la collectivité à veiller à ce que le CSIRT régional propose de manière gratuite les services « de niveau 1) suivants :

- Mise en œuvre d'une plateforme téléphonique et des moyens informatiques nécessaires à la réception des incidents informatiques ;
- Qualification et triage des incidents ;
- Suivi des incidents ;
- Mise en relation avec des prestataires labellisés ExpertCyber (cf. p. 21) ou qualifiés par l'ANSSI ;
- Information et conseil relatifs aux poursuites juridictionnelles ;
- Référencement des prestataires locaux labellisés et qualifiés en cohérence avec l'ANSSI et Cybermalveillance ;
- Relais et transfert des informations pertinentes vers le CERT-FR, CyberMalveillance, les autres CSIRT et l'InterCERT-FR (association nationale des CSIRT et CERT dont l'objectif est de renforcer la capacité de chaque membre à détecter et à répondre aux incidents de sécurité impactant son périmètre) ;
- Consolidation de l'incidentologie régionale et partage du résultat avec le CERT-FR.

Aux côtés du CSIRT régional, **un « Observatoire de la performance cybersécurité des collectivités locales » permettra de proposer aux collectivités franciliennes,** via une prestation confiée à l'entreprise *Board of cyber*, **un diagnostic de risque conçu comme un outil d'appui à la décision pour les maires.** Ces évaluations ne seront pas publiées pour ne pas exposer les collectivités. Il est attendu de l'observatoire une démarche proactive auprès des collectivités les plus exposées au risque pour les sensibiliser et leur proposer des solutions[117].

[117] Audition de Bernard GIRY, 5 septembre 2023.

3.3 La coordination des acteurs est essentielle pour assurer la meilleure protection au territoire francilien

La mobilisation collective prend forme mais peut se heurter à deux écueils : le défaut de prise de conscience des décideurs, nourri par des approches désorganisées. Plusieurs actions sont proposées par les experts entendus dans le cadre de ce rapport :

- **Adopter plusieurs formats de communication fonction des publics concernés, les faire évoluer et les renouveler régulièrement**, pour agir contre la « lassitude », première source de perte de vigilance. En termes de contenu, le témoignage des victimes apparaît essentiel **: il faut promouvoir le droit à l'erreur** et « déculpabiliser » les chefs d'entreprise visés par des cyberattaques, alors qu'un trop grand nombre d'entre eux préfère ne rien en dire en raison du risque réputationnel ;
- **Organiser un ou des évènements « cybersécurité »,** en approchant les chefs d'entreprises sous l'angle de leurs problématiques du quotidien, pour leur présenter à cette occasion les enjeux de sécurité numérique non pas comme une contrainte ou une sanction, mais comme une opportunité : en termes d'amélioration des processus métiers, du processus de production, de préservation de l'innovation, etc. Le format des « Assises de la cybersécurité » organisées en 2018 par la Région pourrait devenir un rendez-vous annuel pour faire connaître (et proposer) de nouvelles solutions concrètes adaptées aux évolutions du risque numérique ;
- **Démultiplier les relais intermédiaires de cette communication** auprès des acteurs concernés : la Région Île-de-France, qui verse des aides à de nombreuses entreprises, associations et collectivités sur le territoire, pourrait participer à cet effort (réseau Île-de-France Entreprises, Club ETI Île-de-France, nouveau réseau des *« développeurs économiques »* régionaux annoncés dans les orientations budgétaires pour 2024[118], etc.).

La Région, si elle n'a bien sûr pas vocation à traiter seule le sujet, est légitime à agir comme **espace d'articulation entre les acteurs de la prévention et de l'intervention sur le territoire régional, dans une approche coordonnée des acteurs économiques et des collectivités** qui en sont les partenaires, pour donner corps à l'ambition inscrite dans son SRDEII : *« L'Île-de-France : un acteur régional de référence en Europe en matière de cybersécurité »*[119].

Le rôle des chambres consulaires et des organisations et fédérations professionnelles, comme celui des têtes de réseaux associatifs, des EPT et des intercommunalités, des syndicats mixtes et des centres de gestion, en appui des réseaux d'élus (Association des maires d'Île-de-France, nouvelle Association des départements d'Île-de-France), apparaît d'autant plus essentiel pour **aborder la sécurité numérique sous l'angle de la prévention, dans un cadre de confiance entre pairs**. S'agissant des TPME seules, la dernière édition du *Baromètre* FranceNum montre qu'une part croissante des chefs d'entreprise se tournent en priorité vers **leurs réseaux professionnels** pour être conseillée (36 % soit + 4 points par rapport à 2022)[120].

Un rapprochement avec la Préfecture de Région, qui dispose notamment des services du délégué régional à l'information stratégique et à la sécurité économiques, **ainsi qu'avec la délégation régionale de l'ANSSI, apparaît utile pour mutualiser les efforts de sollicitation de ces structures-relais.**

Pour le grand public, le réseau des médiathèques et des France Services (anciennement Maisons de services au public), dont plusieurs accueillent d'ailleurs des « conseillers numériques » (CNFS), constituent de bons relais de communication.

[118] Délibération du Conseil régional n° CR 2023-052 adoptée le 16 novembre 2023.
[119] SRDEII 2022-2028, axe 1, sous-axe 1.2 : *« Protéger les TPE, PME et ETI contre l'exposition au risque grandissant de cyber-attaque »,* délibération du Conseil régional n° CR 2022-029, op. cit.
[120] *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023,* FranceNum / Crédoc, op. cit.

Conclusion

Le risque numérique n'est pas une fatalité : s'il n'épargne plus personne (États et administrations, collectivités, établissements publics, entreprises, associations, personnalités et citoyens) des mesures de protection existent, auxquelles la Région Île-de-France prend progressivement part.

L'enjeu est de les **« passer à l'échelle » en accompagnant leur structuration, leur adaptation (aux plus fragiles en particulier) et leur territorialisation**, tout en développant l'information et la formation qui permettent à chacun de réduire son exposition au risque numérique. Il s'agit de se protéger des menaces qui nous sont aujourd'hui connues, mais **c'est aussi un investissement pour l'avenir,** alors que l'intelligence artificielle et l'informatique quantique engagent leur déploiement.

Cet objectif appelle **un effort de coordination** pour assurer « le dernier kilomètre » de service auprès des entreprises, des associations et des collectivités franciliennes. Développer « le réflexe cyber » repose en effet sur la mobilisation de toutes les parties-prenantes : **la cyberprévention est une responsabilité collective, condition pour transformer les risques et défis en atouts ; elle constitue en cela un enjeu de sécurité et de citoyenneté.**

Remerciements

Nous tenons à remercier chaleureusement les personnes auditionnées qui, par leurs expériences et leurs expertises, nous ont aidés à mieux appréhender les enjeux de prévention et de protection des entreprises contre le risque cyber.

Les qualités et fonctions des personnes citées le sont au moment de leur audition par la commission.

- **Agence nationale de la sécurité des systèmes d'information :** Guillaume CRÉPIN, délégué territorial pour la région Île-de-France ;
- **Banque de France :** Julien LASALLE, adjoint au directeur des études et de la surveillance des paiements, secrétaire général de l'Observatoire de la sécurité des moyens de paiement ;
- **Groupe ADIT :** Pierre de BOUSQUET, *senior advisor* ;
- **Centre interdépartemental de gestion de la Grande couronne de la région d'Île-de-France :** Jean-Laurent NGUYEN-KHAC, directeur général ;
- **Cybiah :** Anne-Sophie COLLÉAUX, coordinatrice ;
- **Région Île-de-France :** Bernard GIRY, directeur général adjoint, directeur du pôle Transformation numérique ; Amaël PILVEN, directeur général adjoint, directeur du pôle Entreprises et Emploi ;
- **Conseil régional d'Île-de-France :** Alexandra DUBLANCHE, vice-présidente chargée de la relance, de l'attractivité, du développement économique et de l'innovation.

Liste des membres de la commission Développement économique

Bernard COHEN-HADAD
Président de la commission
Rapporteur

Vincent GAUTHERON
Co-rapporteur

Leila AÏCHI	Errahman GOURARI
Catherine BALAZOT	Yolande GOURNAY
Gérald BARBIER	Jean-Louis HULIN
Christine BESSARD	Catherine LESTERPT
Hervé BIAUSSER	Daniel LEVEL
Patrick BRIALLART	Cécile MARCHAND
Bruno BRISEBARRE	Serge MAS
Michèle CLAYZAC	Christine NEDELEC
Clément DE SOUZA	Reza PAINCHAN
Élisabeth DÉTRY	Vincent PIGACHE
Mireille FLAM	Lionnel RAINFRAY
Stéphanie GASTAUD	Marinette SOLER
Éric GELPE	Sandrine VERRIER

Chargé de mission : Olivier BOURHIS

Glossaire

AAI Autorité administrative indépendante
ACPR Autorité de contrôle prudentiel et de résolution
AMRAE Association pour le management des risques et des assurances de l'entreprise
ANSSI Agence nationale de la sécurité des systèmes d'information
CCI Chambre de commerce et d'industrie
CERT *Computer Emergency Response Team* (cf. p. 29)
CESE Conseil économique, social et environnemental
Ceser Conseil économique, social et environnemental régional
CESIN Club des experts de la sécurité de l'information et du numérique
CIG Centre interdépartemental de gestion
CLOM Cours en ligne ouvert massivement (équivalent français de « MOOC »)
CMQ Campus des métiers et des qualifications
CNFPT Centre national de la fonction publique territoriale
CNFS Conseiller numérique France Services
CNIL Commission nationale Informatique et Libertés
COJO Comité d'organisation des Jeux Olympiques et Paralympiques de Paris 2024
CPME Confédération des petites et moyennes entreprises,
CSIRT *Computer Security Incident Response Team* (cf. p. 39)
DCSSI Direction centrale de la sécurité des systèmes d'information
DGCCRF Direction générale de la concurrence, de la consommation et de la répression des fraudes
DGE Direction générale des entreprises
DPO Délégué à la protection des données personnelles
DRIEETS Direction régionale et interdépartementale de l'économie, de l'emploi, du travail et des solidarités
DSI Directeur des systèmes d'information
EDIH *European Digital Innovation Hub* (cf. p. 34)
ENISA Agence européenne pour la cybersécurité *(European Union Agency for Cybersecurity)*
ENT Environnement numérique de travail
EPCI Établissement public de coopération intercommunale
EPT Établissement public territorial
ETI Entreprise de taille intermédiaire
FEDER Fonds européen de développement régional
GIP Groupement d'intérêt public
IoT Internet des objets (Internet of Things)
MEDEF Mouvement des entreprises de France
OCDE Organisation de coopération et de développement économiques
OIV Opérateur d'importance vitale (définition en p. 5)
OPSN Opérateur public de services numériques
OSE Opérateur de services essentiels (définition en p. 28)
OSMP Observatoire de la sécurité des moyens de paiement (cf. p. 32)
PJL Projet de loi
PME Petite et moyenne entreprise
PTNum Pôle Transformation numérique de la Région Île-de-France (cf. p. 38)
RGPD Règlement général sur la protection des données
RSI Responsable de la sécurité des systèmes d'information
SGDSN Secrétariat général de la défense et de la sécurité nationale
SISSE Service de l'information stratégique et de la sécurité économiques
SRDEII Schéma régional de développement économique, d'innovation et d'internationalisation
SSI Sécurité des systèmes d'information
TPE Très petite entreprise
U2P Union des entreprises de proximité

Bibliographie

Textes législatifs et règlementaires

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE du 4 mai 2016 ;
- Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité), *(Cybersecurity Act),* JOUE du 7 juin 2019 ;
- Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (*Data Governance Act),* JOUE du 3 juin 2022 ;
- Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (*Digital Markets Act*), JOUE du 14 septembre 2022 ;
- Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (*Digital Services Act),* JOUE du 27 octobre 2022 ;
- Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, JOUE du 27 décembre 2022.
- Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques *(European Cyber Resilience Act),* 15 septembre 2022 ;
- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « Directive SRI/2 », JOUE du 27 décembre 2022 ;
- Code des assurances, Livre I^er^ : *Le contrat*, Titre II : *Règles relatives aux assurances de dommages*, Chapitre X : *L'assurance des risques de cyberattaques*, article L12-10-1 ;
- Code de la consommation, Livre I^er^ : *Information des consommateurs et pratiques commerciales*, Titre I^er^ : Information des consommateurs, Chapitre I^er^ : *Obligation générale d'information précontractuelle*, article L111-7-3. ;
- Code monétaire et financier, Livre I^er^ : *La monnaie*, Titre VI : *Dispositions pénales*, Chapitre III : *Infractions relatives aux chèques et aux autres instruments de la monnaie scripturale* (articles L163-1 à L163-12) ; Livre V : *Les prestataires de services*, Titre VII : *Dispositions pénales*, Chapitre I^er^ : *Dispositions relatives aux prestataires de services bancaires* (articles L571-1 à L571-16) ;
- Code pénal, Livre III : *Des crimes et délits contre les biens*, Titre II : *Des autres atteintes aux biens*, Chapitre III : *Des atteintes aux systèmes de traitement automatisé de données,* articles 323-1 à 323-8 ;
- Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite « loi Godfrain », JORF du 6 janvier 1988 ;
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « informatique et libertés », JORF du 7 janvier 1978 ;
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF du 22 juin 2004 ;
- Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF du 19 décembre 2013 ;
- Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, JORF du 14 juillet 2018 ;

- Loi n°2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public, JORF du 4 mars 2022 ;
- Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur, JORF du 25 janvier 2023 ;
- Projet de loi visant à sécuriser et réguler l'espace numérique, texte déposé par M. Bruno LE MAIRE, ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique, déposé au Sénat le 10 mai 2023 (en cours d'examen à la date de rédaction de ce rapport) ;
- Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé Agence nationale de la sécurité des systèmes d'information, JORF du 8 juillet 2009 (modifié par décrets successifs) ;
- Arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance, JORF du 5 mars 2017 (modifié par arrêtés successifs) ;
- Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire de la défense, JORF du 19 septembre 2017 ;
- Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire du droit, JORF du 7 décembre 2018 ;
- Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire du droit, JORF du 31 août 2019 ;
- Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire du droit, JORF du 14 septembre 2021.

Délibérations et actes du Conseil régional d'Île-de-France

- Délibération de la commission permanente du Conseil régional n° CP 2022-123 – *Filière cybersécurité,* adoptée le 23 mars 2022 ;
- Délibération du Conseil régional n° CR 2022-029 – *Schéma régional de développement économique d'innovation et d'internationalisation (SRDEII) 2022-2028*, adoptée le 19 mai 2022 ;
- Délibération de la commission permanente du Conseil régional n° CP 2022-483 – *CERT régional, grands lieux d'innovation, pack quantique*, adoptée le 19 novembre 2022 ;
- Délibération du Conseil régional n° CR 2023-018 – *Budget supplémentaire 2023*, adoptée le 31 mai 2023 ;
- Délibération de la commission permanente du Conseil régional n° CP 2023-246 – *Tiers-lieux et autres affaires économiques*, adoptée le 5 juillet 2023 ;
- Délibération de la commission permanente du Conseil régional n° CP 2023-327 – *Filières et innovation*, adoptée le 21 septembre 2023 ;
- Délibération du Conseil régional n° CR 2023-052 – *Orientations budgétaires pour 2024,* adoptée le 16 novembre 2023 ;
- Délibération de la commission permanente du Conseil régional n° CP 2023-381 – *Filières et innovation*, adoptée le 17 novembre 2023 ;
- Avis d'attribution de marché public n° 23-94497 – *Prestations de déploiement du CSIRT de la Région Île-de-France - Lots 1 à 3*, BOAMP du 7 juillet 2023 ;
- *Appel à manifestation d'intérêt pour le référencement de prestataires cybersécurité (niveau 2) franciliens par le CSIRT Île-de-France*, publié sur le site internet de la Région, consulté le 26 octobre 2023.

Rapports et avis du CESE et des Ceser

- Conseil économique, social et environnemental régional d'Auvergne-Rhône-Alpes, note de sensibilisation – *Cybersécurité : une urgence à se protéger,* présentée par Éric LE JAOUEN, 23 janvier 2019 ;
- Conseil économique, social et environnemental régional d'Île-de-France, rapport et avis n° 2020-15 – *L'Entreprise 4.0 : réussir le passage à l'entreprise du futur,* présenté par Clément DE SOUZA, 15 octobre 2020 ;
- Conseil économique, social et environnemental, avis n° 2022-007 – *Climat, cyber, pandémie : le système assurantiel mis au défi des risques systémiques*, 13 avril 2022 ;

- Conseil économique, social et environnemental régional d'Île-de-France, avis n° 2022-04 – *Schéma régional de développement économique, d'innovation et d'internationalisation (SRDEII) 2022-2028*, présenté par Vincent PIGACHE, 12 mai 2022.

Enquêtes, études et rapports

- Assemblée nationale – *La cyber-assurance*, rapport conduit par Valéria FAURE-MUNTIAN, députée de la Loire et présidente du groupe d'études « Assurances », octobre 2021 ;
- Agence nationale de la sécurité des systèmes d'information, avec Syntec Numérique – *Panorama des métiers de la cybersécurité – Édition 2020,* octobre 2020 ;
- Agence nationale de la sécurité des systèmes d'information, avec l'Agence nationale pour la formation professionnelle des adultes (Afpa) et la délégation générale à l'emploi et à la formation professionnelle du ministère du Travail, de l'Emploi et de l'Insertion – *Les profils de la cybersécurité – Enquête 2021*, septembre 2021 ;
- Agence nationale de la sécurité des systèmes d'information – *Panorama de la menace informatique 2021*, publié le 9 mars 2022 ;
- Agence nationale de la sécurité des systèmes d'information – *Panorama de la cybermenace 2022*, publié le 24 janvier 2023 ;
- Asterès – *Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022*, juin 2023.
- Chambre de commerce et d'industrie Paris Île-de-France – *Pérenniser l'entreprise face au risque cyber : de la cybersécurité à la cyberrésilience*, septembre 2020 ;
- Club des experts de la sécurité de l'information et du numérique (CESIN), étude réalisée par OpinionWay – *Baromètre annuel de la cybersécurité des entreprises*, 8ème édition, publié le 30 janvier 2023 ;
- FranceNum, étude réalisée par le Centre de recherche pour l'étude et l'observation des conditions de vie (Crédoc) – *Le numérique dans les TPME et PME de 0 à 249 salariés – Évolutions entre 2022 et 2023,* publié le 25 septembre 2023 ;
- Grande École du Numérique – *Observatoire GEN_SCAN - Rentrée 2023 : tendances de l'emploi et de la formation au numérique en France,* 2ème édition, publié le 1er octobre 2023.
- Hiscox Assurances, étude réalisée par Forrester Consulting – *Rapport Hiscox 2023 sur la gestion des cyber-risques*, 7ème édition, publié le 10 octobre 2023 ;
- Institut Paris Région, enquête réalisée par l'Ipsos, *Baromètre des Franciliens – Édition 2023*, publié le 12 octobre 2023 ;
- Institut Paris Région, avec l'Insee Île-de-France et la Chambre de commerce et d'industrie Paris Île-de-France – *Chiffres-clés de la région Île-de-France 2023*, juin 2023 ;
- Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique – *Le développement de l'assurance cyber*, publié le 7 septembre 2022 ;
- Ministère délégué chargé de la Transition numérique et des Télécommunications avec l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), l'Agence nationale de la cohésion des territoires (ANCT) et le Conseil général de l'économie (CGE), étude réalisée par le Centre de recherche pour l'étude et l'observation des conditions de vie (Crédoc) – *Baromètre du numérique 2022 : Enquête sur la diffusion des technologies de l'information et de la communication dans la société française*, publié le 30 janvier 2023 ;
- Observatoire prospectif des métiers du numérique, de l'ingénierie, des études et du conseil et des métiers de l'événement (OPIIEC) – *Étude sur les besoins en compétences, emplois et formations de la 5G en France*, juin 2022 ;
- Sénat – *La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?,* rapport d'information fait au nom de la délégation aux entreprises par Sébastien MEURANT, sénateur du Val-d'Oise et Rémi CARDON, sénateur de la Somme, publié le 10 juin 2021 ;
- XEFI, étude réalisée par l'Ipsos – *Enquête : Les TPE/PME et la cybersécurité*, décembre 2021.

Revue de presse

- Cybercriminalité : l'Île-de-France déploie son bouclier défensif, *Les Échos*, publié le 18 novembre 2022 ;

- Cybercriminalité : la Région Île-de-France lance un observatoire de performance, *Affiches Parisiennes*, publié le 24 novembre 2022 ;
- Jean-Noël Barrot missionne le Campus Cyber pour assurer la protection des PME, *cybersecurite-solutions.com*, publié le 28 novembre 2022 ;
- Télétravail : l'Île-de-France championne du travail à distance, *Le Journal du Dimanche*, publié le 21 janvier 2023 ;
- La Région parie sur la cybersécurité, *Le journal du Grand Paris,* publié le 16 mars 2023.
- La Région annonce des mesures pour les entreprises, *Écho d'Île-de-France*, n°1808, semaine du 31 mars au 7 avril 2023 ;
- La Région annonce des mesures pour renforcer sa cybersécurité, *Affiches parisiennes*, publié le 22 mars 2023 ;
- Cyberattaques : face à la menace fantôme, la riposte s'organise, *Le Parisien*, publié le 8 mai 2023 ;
- Assurance cyber : les PME s'assurent plus qu'avant, et elles vont bientôt le regretter, *L'Usine digitale*, publié le 24 mai 2023 ;
- Cybersécurité : les structures mutualisantes peinent à enrôler les maires des petites communes, *La Gazette des Communes*, publié le 6 octobre 2023.

Communiqués de presse

- Agence nationale de la sécurité des systèmes d'information – *Centres régionaux de réponse à incident cyber : création des structures dans sept régions*, publié le 11 janvier 2022 ;
- Agence nationale de la sécurité des systèmes d'information – *MonServiceSécurisé : l'ANSSI lance une nouvelle solution pour sécuriser et homologuer les services publics en ligne,* publié le 13 mars 2022 ;
- Région Île-de-France – *La Région Île-de-France annonce plusieurs mesures en matière de cybersécurité,* publié le 14 mars 2023 ;
- Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique – *L'Observatoire de la sécurité des moyens de paiement émet des recommandations sur le remboursement des victimes de fraude***,** publié le 16 mai 2023 **;**
- **Région Île-de-**France **–** *À Viva Technology, du nouveau pour que l'Île-de-France reste la 1ère Smart Région d'Europe*, publié le 15 juin 2023.

Guides pratiques

- **Agence** nationale de la sécurité des systèmes d'information, en partenariat avec la direction des affaires criminelles et des grâces du ministère de la Justice – *Attaques par rançongiciels, tous concernés : comment les anticiper en cas d'incident ?*, septembre 2020 ;
- **Agence** nationale de la sécurité des systèmes d'information, en partenariat avec le Club de la continuité d'activité – *Organiser un exercice de gestion de crise cyber,* octobre 2020 ;
- **Agence** nationale de la sécurité des systèmes d'information, en partenariat avec Cap'Com – *Anticiper et gérer sa communication de crise cyber,* décembre 2021 ;
- **Agence** nationale de la sécurité des systèmes d'information, en partenariat avec la direction générale des entreprises, la Confédération des petites et moyennes entreprises (CPME) et FranceNum - *La cybersécurité pour les TPE/PME en treize questions*, octobre 2022 ;
- Centre interdépartemental de gestion Grande couronne de la région d'Île-de-France – *Cyberattaque - Gérer la crise, se reconstruire et se protéger,* juillet 2023 ;
- **CyberMalveillance**, en partenariat avec BpiFrance – *Guide de cybersécurité à destination des dirigeants de TPE, PME et ETI,* mai 2021 ;
- **CyberMalveillance**, en partenariat avec la Commission nationale Informatique et Libertés (CNIL) – *Les obligations et responsabilités des collectivités locales en matière de cybersécurité,* juillet 2022 ;
- **CyberMalveillance**, en partenariat avec l'Association des maires de France – *Méthode clé en main pour sensibiliser les agents des collectivités*, novembre 2022 ;
- **CyberMalveillance** – *Cyber Guide Famille : 10 bonnes pratiques essentielles pour protéger les usages numériques de la famille*, octobre 2023.

Autres

- Premier ministre – *Stratégie nationale pour la sécurité du numérique*, juin 2015 ;
- Gouvernement – *Stratégie nationale d'accélération pour la cybersécurité*, 18 février 2021.

Sitographie

- campuscyber.fr : site internet du Campus Cyber (La Défense) ;
- cert.ssi.gouv.fr : site internet du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) ;
- cybermalveillance.gouv.fr : site internet du GIP Agir contre la cybermalveillance (Acyma) ;
- grandeecolenumerique.fr : site internet du GIP Grande École du Numérique et ressources en ligne de l'Observatoire GEN_SCAN de l'emploi et la formation au numérique ;
- Observatoire de la sécurité des moyens de paiement, Banque de France ;
- Portail internet des aides et appels à projets de la Région Île-de-France ;
- Pix, service public en ligne d'évaluation et de certification des compétences numériques ;
- SecNum*académie* : cours en ligne ouvert massivement (CLOM) proposé par le centre de formation à la sécurité des systèmes d'information de l'Agence nationale de la sécurité des systèmes d'information ;
- SensCyber : programme en ligne de sensibilisation à la cybersécurité, destiné à tous les agents de la fonction publique, proposé par CyberMalveillance et développé avec le ministère de la Transformation et de la Fonction publiques, la direction générale de l'administration et de la fonction publique (DGAFP), le Centre national de la fonction publique territoriale (CNFPT) et l'Association nationale pour la formation permanente du personnel hospitalier (ANFH) ;
- Portail internet des aides et appels à projets de la Région Île-de-France ;
- ssi.gouv.fr : site internet de l'Agence nationale de la sécurité des systèmes d'information.

Annexes

CharteCyber proposée par CyberMalveillance et signée par la Région Île-de-France

Du diagnostic à l'investissement : deux chèques Cyber

Chèques Cyber Diagnostic

Pour anticiper et se protéger face au risque Cyber grandissant, le chèque Cyber « diagnostic » soutient les dirigeants qui s'engagent dans des démarches de **diagnostic Cyber** et de définition d'un **plan d'actions Cyber détaillé.**

Cible : Les PME franciliennes, entre 10 et 249 salariés, quelle que soit leur forme juridique, y compris les associations ayant une activité économique.

Points clés de l'offre
Financement de prestations de diagnostic :
- audit technique et organisationnel
- audit de conformité, audit d'architecture
- exercice de crise et audit de plan de continuité
- rapport de vulnérabilités
- **→ plan d'actions, feuille de route et priorisation selon criticité / complexité…**
- **Une subvention pouvant aller jusqu'à 5 000 € (le taux d'intervention de la Région est de 80% maximum).**

Quelles démarches ?
Le dossier complet est à déposer sur mesdemarches.iledefrance.fr.

Plus d'informations : www.iledefrance.fr/cheque-diagnostic-cyber

Chèque Cyber Equipement

Afin d'accélérer le passage du diagnostic à l'investissement, la Région soutient les PME qui veulent **investir dans les outils de protection Cyber** avec le chèque Cyber « équipement »

Cible : Les PME franciliennes, entre 10 et 249 salariés, quelle que soit leur forme juridique, y compris les associations ayant une activité économique.

Points clés de l'offre :
- Prérequis : avoir réalisé un diagnostic Cyber

Financement des dépenses d'investissements :
- Les mesures de protection réseau
- Les mesures de mise en conformité aux règlements RGPD, RGS et NIS 2
- Les solutions de protection des sites et applications web
- Les solutions de Cyber veille
- Les scanners de vulnérabilité
- Les évolutions technologiques de l'environnement informatique et/ou les mises à jour logicielles et systèmes
- Les investissements matériels
- **Une subvention pouvant aller jusqu'à 10 000 € (taux d'intervention Région de 50% maximum)**

Quelles démarches ?
Le dossier complet est à déposer sur mesdemarches.iledefrance.fr.

Région îledeFrance

Conseil économique, social et environnemental régional d'Ile-de-France
2, rue Simone Veil • 93 400 Saint-Ouen • Tél. : 01 53 85 66 25
www.ceser-iledefrance.fr • @ceseridf