Cette action bénéficie de l'expertise et du soutien financier du ministère du travail, dans le cadre de l'EDEC des branches du commerce et de la distribution

Cyberdiag TPE-PME

l'opcommerce Opérateur de compétences

Observatoire prospectif du commerce

Rapport d'expérimentation du Cyberdiag

EDEC Commerce 2017-2020

Axe 3 – Cybersécurité

Fiche Action 8 – Cyberdiag

Rapport rédigé par Phosforea en mai 2020

Sous la direction de la Direction Offre de Service et Innovation de l'Opcommerce

PREAMBULE

L'ambition de l'expérimentation Cyberdiag, présentée en détail dans ce rapport, se résume en quelques mots : constater, faire constater et amorcer une prise de conscience sur le nécessaire accompagnement des TPE/PME face aux menaces grandissantes d'un monde numérique hyperconnecté.

Les TPE/PME constituent une part considérable de l'économie française, tant en termes d'emploi, que de richesse créée ou d'investissement en recherche et innovation. Concentrées dans la gestion de leurs affaires courantes, et engagées à 100% dans la réalisation de leur cœur de business, elles ignorent, souvent par manque de temps, le risque numérique qui pourtant, avec la généralisation de l'outil Internet, frappe à leur porte.

Ce contexte de transformation numérique a fortement impacté les entreprises du commerce, aussi est-ce pour cette raison que les 13 branches du Commerce et de la Distribution, le Ministère du Travail et le Forco (devenu l'Opcommerce en avril 2019) en tant qu'organisme relais, ont signé en octobre 2017, l'EDEC Commerce (Engagement Développement Emploi Compétences) ayant pour fil rouge le numérique.

Dans le cadre de cet EDEC, Phosforea, filiale du groupe SCASSI, a été sélectionné pour la réalisation de la fiche-action 8 'Diagnostic Accompagnement cybersécurité Cyberdiag' visant à concevoir un diagnostic pour évaluer l'organisation SI de l'entreprise et sa capacité à se protéger des cyber-attaques puis à l'accompagner dans le renforcement de sa cybersécurité.

La mission, menée sur une durée totale de 10 mois, a permis de mettre au point une démarche coordonnée d'identification, de diagnostic approfondi, de conception de plan d'action et d'accompagnement des TPE/PME vers une plus grande protection de leurs entreprises face aux cyber-menaces.

Cette expérimentation a pu être menée grâce aux savoir-faire conjugués d'une équipe pluridisciplinaire composée d'ingénieurs en pédagogie et d'experts en cybersécurité.

Ce rapport expose le contexte cybersécurité des TPE/PME, le contexte du projet les différents outils créés et la démarche associée, et enfin une synthèse globale et des préconisations.

Vous trouverez ci-dessous, le lexique des termes à connaitre pour lire ce rapport.

Bonne lecture !

LEXIQUE

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.

Cryptovirus : Virus informatique envoyé par des personnes malveillantes dans le but de chiffrer tout ou partie des fichiers présents sur un ordinateur pour les rendre inaccessibles. L'utilisateur est ensuite invité à payer une rançon en échange d'une clé de déchiffrement.

Cyber : préfixe faisant référence à toutes les techniques liées à la société du numérique et notamment à l'informatique et à l'Internet.

Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. (Source : ANSSI).

Malware : logiciel malveillant.

PASSI : Prestataire d'Audit de la Sécurité des Systèmes d'Information.

Phishing (ou hameçonnage) : Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime. (Source : ANSSI).

Ransomware : Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Le terme « rançongiciel » (ou ransomware en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. (Source : ANSSI).

RGPD : « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne. Ce règlement européen d'avril 2016 et entré en vigueur en mai 2018, s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant. Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs. (Source : CNIL).

SI (Systèmes d'Information) : Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un ordinateur. (Source : Wikipedia).

SSI : Sécurité des Systèmes d'Information.

SOMMAIRE

1. TPE/PME ET CYBERSECURITE

1.1 Cybersécurité : un enjeu national

"Tous connectés, tous impliqués, tous responsables", voici le slogan avec lequel l'ANSSI introduit son action auprès de ses abonnés sur le réseau social LinkedIn.

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est l'autorité nationale créée en 2009 pour assurer un service de protection, veille, détection, alerte et réaction aux attaques informatiques. Dans un monde numérique toujours plus connecté, son action est centrale pour assurer la sécurité de l'Etat et des Organismes d'Importance Vitale (OIV), mais aussi pour sensibiliser et accompagner la montée d'une culture numérique chez les acteurs économiques, en particulier les entreprises.

La plateforme en ligne www.cybermalvaillance.gouv.fr a recensé en 2019 pas moins de 90.000 demandes d'aides de la part de victimes d'attaques informatique (contre 28.855 en 2018, soit une augmentation de plus de 210%). Parmi ces victimes, 90% sont des particuliers, souvent plus vulnérables et désarmés face aux incidents de sécurité qui les frappent.

Il en va de même pour les TPE et PME qui, à l'instar des particuliers, ne savent pas souvent vers qui se tourner en cas d'incident informatique. Et les menaces sont toujours plus nombreuses…

Le rapport d'activité 2019 de www.cybermalvaillance.gouv.fr (site de l'Etat d'assistance aux victimes de cyber-malveillances) fait apparaitre les typologies de menaces suivantes, prédominantes en France dans les entreprises :

- l'hameçonnage (phishing) à 23%,
- le piratage de compte à 16%.

Le leader américain du secteur des télécommunications VERIZON quant à lui, fait apparaitre dans sa dernière étude *Verizon 2019 Data Breach Investigations Report (DBIR)*, que **43% des cyberattaques perpétuées dans le monde visent les petites entreprises.**

La cyberguerre n'est pas une fiction, elle a bel et bien commencé comme l'annonçait La Ministre de La Défense en janvier 2019 lors de la présentation de la doctrine offensive sur l'Internet de l'armée française.

Les nouveaux outils numériques et les nouvelles pratiques qui en découlent font peser de nouveaux risques sur les entreprises, notamment sur la protection de leurs données. La multiplication du recours aux outils informatiques induit une profonde évolution des mentalités au sein des TPE/PME.

Dans ce contexte, les acteurs économiques ne peuvent pas ignorer la menace que représente la cybermalveillance :

- Les grandes entreprises ont depuis longtemps pris les devants, en consacrant une part importante de leur **budget à la cybersécurité car en effet, l'ANSSI recommande d'y dédier 5 à 10% du budget global de l'entreprise** ;
- Les PME, font souvent face à une réalité économique ne permettant pas d'atteindre ce niveau d'investissement ;
- Quant aux TPE, d'autres difficultés se conjuguent comme le manque de moyens humains et la faible prise de conscience des risques encourus.

Et pour toutes ces entreprises, il existe un besoin bien réel et commun de développer les compétences car leurs salariés sont leur première source de défense, sous réserve qu'ils signalent le moindre événement qui éveille leurs soupçons : la sensibilisation et la formation à la Sécurité Informatique sont des axes majeurs.

1.2 Développer les compétences en cybersécurité des TPE/PME

1.2.1 Le contexte

Sur la base de la définition de l'INSEE[1] :

- La TPE (Très Petite Entreprise) compte moins de 10 collaborateurs. Elle réalise un chiffre d'affaires inférieur ou égal à 2 millions d'euros ;
- La PME (Petite et Moyenne Entreprise) compte moins de 250 collaborateurs. Elle réalise un chiffre d'affaires inférieur ou égal à 50 millions d'euros ou un bilan inférieur ou égal à 43 millions d'euros.

Les PME constituent d'après l'INSEE 99,90% des entreprises en France, pour 1/3 du chiffre d'affaires total des entreprises françaises[2] et au total, 9% du PIB français. Elles emploient près de la moitié de la masse salariale en France, soit 49% des 14 millions d'actifs du pays. Elles investissements au total plus de 7 milliards d'euros pour la R&D (Recherche & Développement), soit un quart des dépenses totales des entreprises françaises en Recherche et Innovation.

Pour toutes ces raisons, ces entreprises, malgré leur petite taille, constituent des cibles de choix et sont tout autant visées par les cyber-attaques que les grandes entreprises, voire plus…

La situation est plutôt inquiétante pour les TPE/PME : selon la Revue de la Gendarmerie Nationale, **74% des TPE-PME ont déjà pâti d'une cyberattaque**. Le type d'attaque la plus

[1] https://www.insee.fr/fr/metadonnees/definition/c1962

[2] Baromètre des TPE/PME dans l'économie française en 2019, Les Echos, 21 janvier 2020 <https://solutions.lesechos.fr/compta-gestion/c/barometre-des-tpe-pme-dans-leconomie-francaise-en-2019-19385/>

subie reste la demande de rançon (Ransomware), (80%), viennent ensuite les attaques par déni de service (40%), les attaques virales généralisées (36%) et la fraude externe (29%). Paradoxalement, **83% des entreprises se sentent peu ou pas exposées aux risques cyber** ! Ce décalage de perception montre le risque encouru[3].

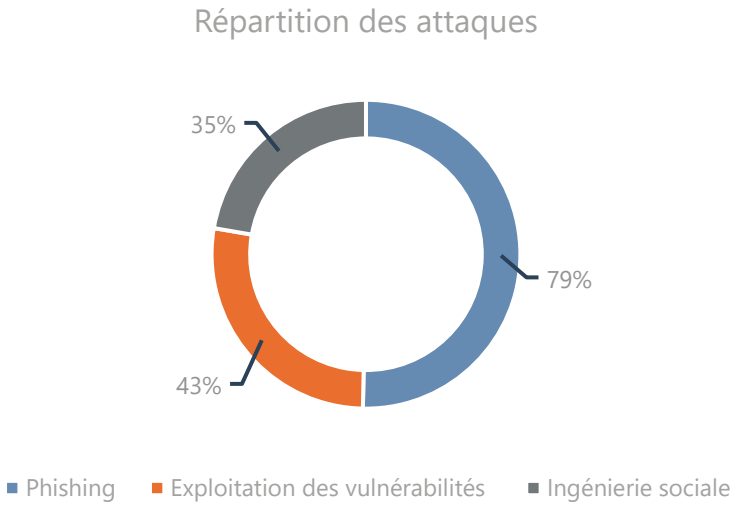
Face à toutes ces menaces, il apparait évident que la première des barrières pour protéger l'entreprise des cyber-attaques reste l'humain. Un personnel sensibilisé, conscient des menaces et des risques pour son entreprise constitue un pare feu important. C'est d'ailleurs dans ce sens que l'ANSSI recommande vivement aux entreprises de former leurs collaborateurs en mettant à leur disposition un MooC (cours en ligne ouvert) pour rendre accessibles les notions clés de la cybersécurité : *la SecNumAcadémie*.

Le site de l'ANSSI précise d'ailleurs : *« La Cybersécurité constitue aujourd'hui un enjeu économique majeur pour les organisations de toutes tailles, notamment les TPE/PME, réputées plus vulnérables que leurs consœurs de grande taille ».*

1.2.2 La menace numérique et les risques pour les TPE/PME

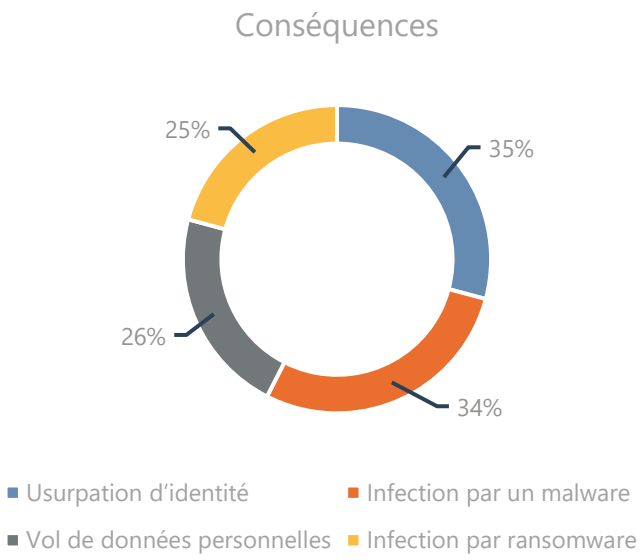
Selon l'enquête CESIN 2020, 8 entreprises sur 10 ont déclaré avoir subi une cyber-attaque en 2018 (source : CESIN).

Répartition des attaques par type : le phishing est largement en tête des menaces.

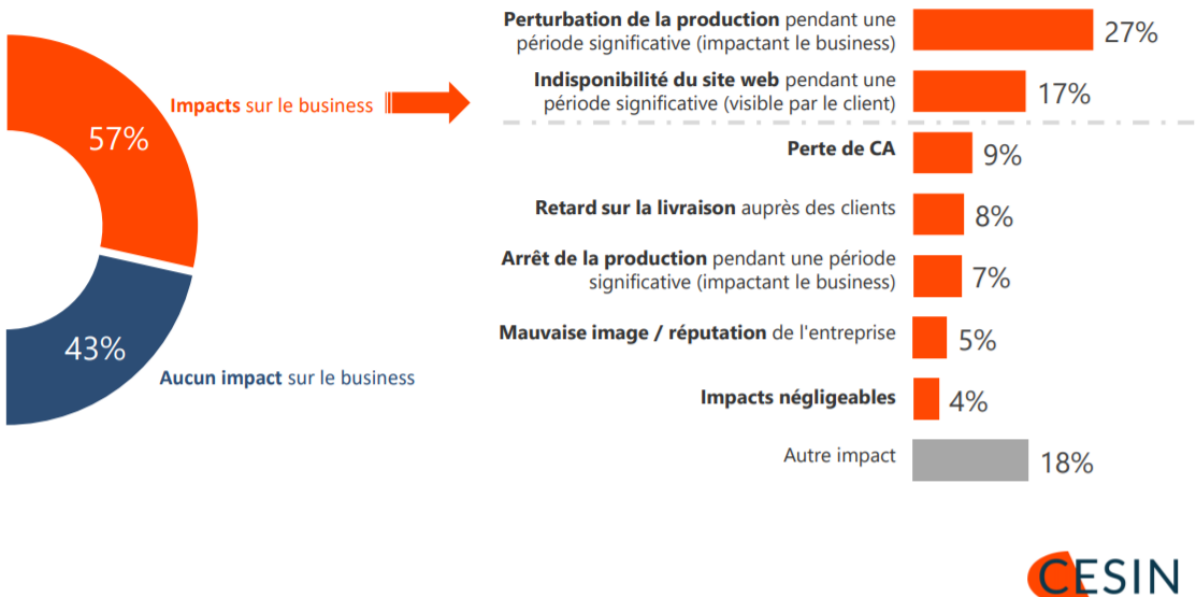


[3] Revue de la Gendarmerie Nationale, avril 2019, n°264 - La sécurité économiques des TPE et des PME

Conséquences des attaques sur les entreprises :



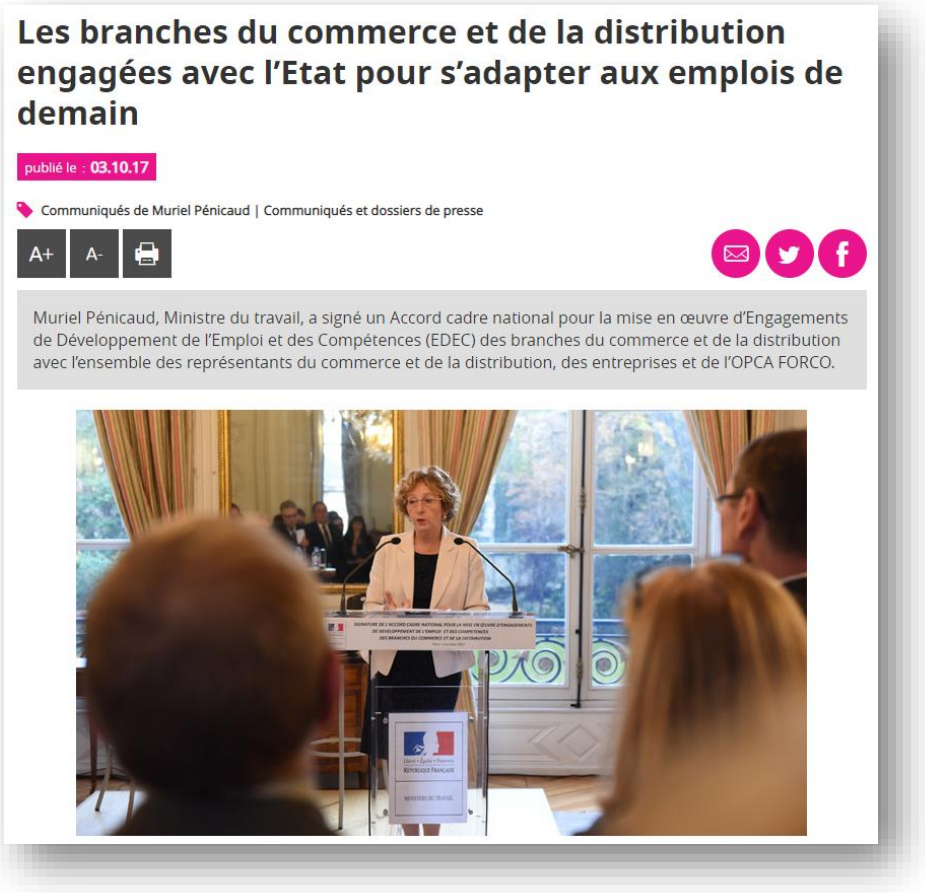
Impact des attaques sur le business : perturbation de la production dans 27% des cas et perte de Chiffre d'Affaires dans 9% des cas.



D'une manière générale, toujours selon l'enquête du CESIN, seules 4 entreprises sur 10 se disent préparées en cas de cyber-attaque de grande ampleur.

1.2.3 Un accompagnement de proximité initié dans le cadre de l'EDEC Commerce

Le 3 octobre 2017, les treize branches professionnelles du Commerce et de la Distribution ont signé un EDEC (Engagement de Développement des Emplois et des Compétences)[4] avec le Ministère du Travail et le Forco (devenu l'Opcommerce) en tant qu'organisme relais. Cet accord-cadre prévoyait en son axe 3 'd'outiller les entreprises pour le développement de la cybersécurité et faire évoluer les compétences'.



Les branches du commerce et de la distribution engagées avec l'Etat pour s'adapter aux emplois de demain

publié le : 03.10.17

Communiqués de Muriel Pénicaud | Communiqués et dossiers de presse

A+ A-

Muriel Pénicaud, Ministre du travail, a signé un Accord cadre national pour la mise en œuvre d'Engagements de Développement de l'Emploi et des Compétences (EDEC) des branches du commerce et de la distribution avec l'ensemble des représentants du commerce et de la distribution, des entreprises et de l'OPCA FORCO.

En effet, l'EDEC Commerce est construit autour de 3 axes :

- L'axe 1 visant à analyser l'impact de la transformation digitale sur les emplois et les compétences dans les branches du Commerce et de la Distribution,
    - Bouleversement des organisations par le **commerce connecté**, l'omnicanalité, changement d'état d'esprit individuellement pour changer de culture collectivement ;

[4] *Source : https://travail-emploi.gouv.fr/actualites/presse/communiques-de-presse/article/les-branches-du-commerce-et-de-la-distribution-engagees-avec-l-etat-pour-s)*

- L'axe 2 visant à accompagner les entreprises dans leurs transformations et leurs stratégies en ressources humaines
    - La transformation humaine poussée par le digital, fidélisation des salariés, RSE, QVT, l'entreprise apprenante…
- L'axe 3 visant à outiller les entreprises pour le développement de la cybersécurité et faire évoluer les compétences'
    - Depuis plusieurs années des cyberattaques en évolution constante, un monde numérique incontournable : de nouveaux outils, de nouvelles pratiques, de nouveaux réflexes visant à protéger l'utilisateur, l'entreprise, l'économie.

Au sein de cet axe 3 dédié à la cybersécurité, 3 fiches action dont la fiche action 8 'Diagnostic accompagnement cybersécurité : Cyberdiag'. Celle-ci visait la conception d'un diagnostic pour évaluer l'organisation SI des entreprises et leur capacité à se protéger des cyber-attaques et un accompagnement dans le renforcement de leur cybersécurité.

Cette fiche action a fait l'objet d'un appel à proposition en décembre 2018.

L'objectif sous-jacent de ce 'Cyberdiag' est aussi de faire prendre conscience aux TPE/PME de l'importance de la cybersécurité, et de les accompagner dans la co-construction d'un plan d'actions qu'elles pourront mettre en œuvre. Un **cahier des charges validé par le COTECH** (COmité TECHnique composé de l'Etat, des 8 branches professionnelles impliquées sur cette fiche action et de l'Opcommerce), a permis de sélectionner un prestataire pouvant construire et mener à bien ce projet sous forme d'expérimentation visant à produire une offre de service par l'Opcommerce pour le compte de ses entreprises adhérentes.

Les 8 branches impliquées dans cette action sont :

- **Bricolage,**
- **Commerce à distance,**
- **Commerce à prédominance alimentaire (détail et gros),**
- **Commerce de détail de l'horlogerie-bijouterie,**
- **Commerce succursaliste de la chaussure,**
- **Import-Export,**
- **Optique-lunetterie de détail,**
- **Professionnels de la photographie.**

Forte de son expérience dans le domaine de la formation et de la cybersécurité, avec l'appui du groupe SCASSI dont elle fait partie, l'entreprise Phosforea s'est portée candidate pour mener à bien ce projet de 'Cyberdiag'.

1.2.4 L'engagement de Phosforea pour l'accompagnement des TPE/PME

Phosforea est un centre de formation expert en cybersécurité. Il crée et déploie des contenus pédagogiques de sensibilisation et de formation, adaptés à la transmission de savoirs et de savoir-faire en cybersécurité. Avec une expérience de 15 années, auprès de plus de 70 clients en Europe, la société dispose d'un solide savoir-faire en matière de formation à la sécurité des systèmes d'information (SSI). Elle propose des contenus, parcours de formation et supports adaptés aux besoins spécifiques de ses clients. Phosforea accompagne depuis sa création des entreprises de toutes tailles, depuis le grand groupe international, jusqu'à la PME locale.

Phosforea a conçu le MOOC de l'ANSSI, la SecNum académie[5], en développant 4 modules e-learning en cybersécurité découpé en 5 unités de 1h20 chacun.

Le projet de R&D qui a donné naissance à Phosforea en 2017, intitulé Risky Knowledge est soutenu par l'Union européenne dans le cadre du programme Leonardo Da Vinci. Il a permis de dégager une cartographie complète de la compétence en cybersécurité applicable à tout type de contexte professionnel et toutes tailles d'entreprises.

Phosforea a été retenu à l'issu de 2 auditions pour mener à bien le projet Cyberdiag.

1.2.5 Phosforea et le Groupe SCASSI : une équipe pluridisciplinaire d'experts

L'un des atouts de Phosforea, filiale du groupe SCASSI, réside dans la force de ce groupement.

La société SCASSI est un pure player de la cybersécurité, spécialisé dans la protection des systèmes d'information critiques et embarqués. Elle est qualifiée Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI), attestant de la conformité aux exigences règlementaires, techniques et de sécurité promue par l'ANSSI et apportant une garantie de compétence.

La compétence et l'expérience de ses ingénieurs et experts en sécurité informatique permettent d'apporter une plus-value à la formation, à son contenu et l'accompagnement des entreprises.

La combinaison du savoir-faire de ces deux entreprises (pédagogie et cybersécurité) permet d'apporter une véritable complémentarité et une expertise dans leurs missions respectives.

Présentation de l'équipe Phosforea

L'équipe Phosforea est constituée de profils variés, complémentaires dans leurs compétences et savoir-faire :

[5] https://secnumacademie.gouv.fr/

- Ingénieurs pédagogiques, experts de la conception et mise au point de contenus de formation,
- Infographistes spécialisés dans le design,
- Développeurs web,
- Chefs de projet.

Ce dernier profil a été la clé dans la gestion et le pilotage de cette expérimentation. Les compétences pluridisciplinaires et de coordination d'équipe ont permis de garantir la tenue des délais dans le respect de la qualité qu'une telle expérimentation exige.

L'accompagnement des entreprises, de l'audit à la co-construction du plan d'action, a été mené quant à lui par les ingénieurs sécurité de SCASSI.

La diversité des talents de la société SCASSI, regroupant ingénieurs, juristes et consultants, a permis d'assurer :

- La fiabilité de la méthode de diagnostic proposé,
- La pertinence des rapports remis aux entreprises,
- La pertinence de l'accompagnement mis en place.

En synthèse, l'addition des savoir-faire de Phosforea et se SCASSI ont été un facteur clé de succès pour cette expérimentation.

2. Proposition de structure du Cyberdiag

2.1 Un projet en 4 phases

Le choix du prestataire ainsi que les orientations du projet ont été orientés, validés par le COTECH composé des acteurs-clés suivants :

- Les 8 branches professionnelles participantes,
- La DGEFP,
- L'Opcommerce,
- L'Observatoire Prospectif du Commerce,
- Le prestataire (Phosforea à compter de sa sélection pour le projet).

Tout au long du projet, le COTECH s'est réuni périodiquement afin de suivre l'avancement des travaux, voire de les ajuster le cas échéant, et d'en valider les différentes étapes.

Pour mémoire, le Cyberdiag doit permettre dans un premier temps, de faire un état des lieux de la sécurité informatique des entreprises des 8 branches professionnelles impliquées et d'évaluer leur capacité à résister et à se prémunir des cyber-attaques ; puis à les accompagner à renforcer leur capacité de résistance.

Dans le cadre de l'EDEC Commerce, le projet étant totalement cofinancé par l'Opcommerce et l'Etat, aucune participation financière n'est demandée aux entreprises participantes sur la durée de l'expérimentation.

Dans sa réponse à l'appel à propositions, en mars 2019, Phosforea a proposé un diagnostic cybersécurité par une approche pragmatique et accompagnante en direction des entreprises. Cette démarche est scindée en quatre phases pour mener à bien l'expérimentation du Cyberdiag. Celle-ci est adaptée aux différentes typologies d'entreprises, en tenant compte de leur taille et des spécificités des branches professionnelles impliquées qu'elles représentent.

Vous trouverez en suivant le découpage initialement proposé par Phosforea, et retenu par le COTECH.

Cyberdiag : un projet en 4 phases

(Validation du COTECH du 27 mars 2019)

Phase 1 : Identification des pratiques cybersécurité des TPE/PME

- Cibler des entreprises
- Communiquer et sensibiliser les entreprises sur la démarche
- Acquérir du contexte et des pratiques à travers divers canaux

Phase 2 : Construction du diagnostic orienté Commerce et Distribution

- Rédiger et établir un cadre méthodologique et outillé pour la réalisation du diagnostic

Phase 3 : Test du diagnostic

- Tester le diagnostic auprès d'un panel d'entreprises
- Présenter des préconisations au dirigeant d'entreprise pour être échangées ou validées
- Co-construction d'un plan d'actions selon les préconisations
- Appel de suivi par un consultant un mois après la prestation
- Questionnaire de satisfaction entreprise

Phase 4 : Restitution

- Rédiger un rapport final avec des préconisations ciblées par branche

► ***Ajustement :***

Au vu des contraintes rencontrées pendant le déroulement du projet, les phases ont été remaniées afin d'assurer un déroulé opérationnel cohérent et dans les temps impartis :

- La phase 1 a pu être réalisée ;
- Les phases 2 et 3 ont été fusionnées : la sélection des entreprises ayant été plus difficile que prévu la temporalité en a été raccourcie.

2.1.1 Phase 1 : Identification des pratiques Cybersécurité des TPE/PME

La phase 1 de la mise en œuvre du projet se résume à trois objectifs principaux :

- **Communiquer** (promotion du Cyberdiag) vers les entreprises des branches impliquées,
- **Identifier des entreprises** désireuses de participer l'expérimentation (tester le Cyberdiag),
- **Acquérir de la connaissance** sur l'environnement, les risques et les spécificités propres aux entreprises du Commerce et de la Distribution.

2.1.1.1 Communiquer

La communication est le point de départ de cette expérimentation. Elle vise à informer les entreprises de l'existence du projet ainsi que des détails inhérents à celui-ci mais également à les inviter à participer à l'expérimentation.

Pour ce faire, Phosforea a préconisé plusieurs canaux de communication promotionnels (Internet…), complétés par des outils plébiscités par les branches au regard des pratiques de leurs entreprises (triptyque) et aussi pour la promotion du Cyberkit via les réseaux sociaux et conseillers emploi/formation de l'Opcommerce (vidéo).

Ces supports promotionnels sont également des outils d'aide au recrutement des entreprises pour les branches professionnelles et pour les conseillers de l'Opcommerce. Ils apportent un éclairage détaillé de l'expérimentation, tant au niveau du service proposé que de sa temporalité.

Identité visuelle du Cyberdiag

Dès le début du projet, il est apparu important que l'expérimentation soit clairement identifiable aussi bien par les membres du COTECH, les conseillers emploi-formation de l'Opcommerce, les entreprises des branches impliquées, que par le grand public (dans le cadre de l'EDEC Commerce). L'intitulé Cyberdiag initialement proposé dans l'EDEC Commerce a été validé par les membres du COTECH, celui-ci résumant bien l'objectif de la démarche.

Un logo dédié au Cyberdiag a été proposé et est apposé sur tous les documents et supports de communication en lien avec l'expérimentation.

Logo dédié au Cyberdiag
(COTECH du 11 avril 2019)

Un site internet dédié

La proposition de Phosforea de créer un site internet dédié à l'expérimentation a été retenue. Les membres du COTECH ont néanmoins décidé du nom de domaine retenu : https://www.cyberdiag-tpe-pme.com

Page d'accueil du site https://www.cyberdiag-tpe-pme.com

Le site internet est composé de 2 parties :

- **Une vitrine donnant une description détaillée du Cyberdiag.**
  Au-delà de la promotion plus large du projet, ce point du plan de communication donne du crédit au projet.
  En effet, le site internet est un élément tangible matérialisant la démarche : il est un gage de confiance pour les entreprises participantes car il est un élément de validation de l'existence du projet.

  Les rubriques vitrines du site Internet sont les suivantes :

  - Page d'accueil avec un bouton s'identifier,
  - Présentation du projet,
  - Les services liés au Cyberdiag,
  - Le calendrier du projet,
  - Les porteurs du projet,
  - Une rubrique contact.
    Cette rubrique permet à toute personne intéressée par le projet, de compléter un formulaire de contact pour :
    - demander des informations,
    - demander à participer au Cyberdiag,
    - contacter le support technique.

    Ce formulaire est relié à une adresse email dédiée – contact@cyberdiag-tpe-pme.com – qui permet une prise de contact avec Phosforea qui relaye l'information à l'Opcommerce.

Sur la durée de l'expérimentation *(9 mois)*, une dizaine d'entreprises ont demandé à participer à l'expérimentation. Deux d'entre elles étaient éligibles et y ont participé car relevant des branches professionnelles impliquées.

Cyberdiag – Site Internet rubrique *Présentation du projet*

- **Un espace personnel sécurisé**
  Cet espace personnel sécurisé est matérialisé par un bouton *'s'identifier'* en haut à droite de chaque page de la vitrine.
  Il héberge des outils et ressources liées au Cyberdiag. Son accès se fait au travers de codes communiqués par Phosforea aux entreprises entrant dans l'expérimentation.
  Cet espace est central dans la démarche car il héberge de manière sécurisée des outils nécessaires à plusieurs étapes du projet :
  - L'Autodiag (cf. 2.1.2.2),
  - Les tutos (guides des bonnes pratiques, cf 2.1.2.2),
  - Le questionnaire d'évaluation (cf 2.1.2.3).

Cyberdiag : Site Internet Espace personnel sécurisé

La fréquentation sur le site internet a été de 418 visites venant de 200 utilisateurs différents sur la durée de l'expérimentation *(juin 2019 à mars 2020)*.

Un triptyque à destination des entreprises

Afin de présenter aux entreprises des branches impliquées, l'expérimentation et la démarche de manière pragmatique et synthétique, **un triptyque a été proposé à la demande des branches.** Ce triptyque a été transmis sous format digital aux membres du COTECH afin d'assurer la promotion de l'opération.

Triptyque de promotion du Cyberdiag

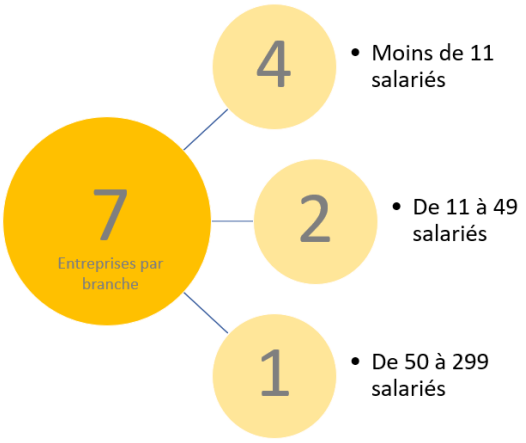
Une vidéo pédagogique et promotionnelle du Cyberdiag

Afin de compléter la communication du Cyberdiag, **une vidéo d'une durée de 2 minutes** détaillant l'offre et la démarche est en cours de création. Elle viendra en appui de l'offre de service proposée par l'Opcommerce.

2.1.1.2 Identifier des entreprises

Il a été proposé d'expérimenter le Cyberdiag sur 56 entreprises réparties sur les 8 branches professionnelles participantes, soit 7 entreprises par branche. La distribution par taille d'entreprise a été validée en COTECH afin de favoriser la représentativité des entreprises de moins de 11 salariés comme le spécifiait l'appel à projets.

Cyberdiag : sélection des entreprises
(Validation du COTECH de cadrage du 11 avril 2019)



Lors du COTECH du 11 avril, la répartition des entreprises par taille a été actée ainsi que le recrutement des entreprises par les branches professionnelles impliquées, pour le mois suivant. Les coordonnées des participants à l'expérimentation ont été transmises au prestataire via l'Opcommerce.

► ***Ajustement***

Des difficultés de recrutement ont décalé dans le temps l'opération Cyberdiag.

2.1.1.3 Acquérir de la connaissance

L'objectif de cette phase est **d'acquérir de la connaissance** sur l'environnement, les risques et les spécificités propres aux entreprises des branches impliquées et de constater s'il existe une empreinte Commerce en matière de Cybersécurité. De plus, cette acquisition de contexte permet de disposer d'un état des lieux représentatif permettant la formation d'hypothèses et abaques permettant la construction du diagnostic.

Pour ce faire, la phase d'acquisition de contexte se focalise sur :

- L'environnement informatique (architecture, modalités d'exploitation),
- Les usages faits des moyens informatiques (systèmes de caisses, logiciels de gestion d'entreprise ou de gestion comptable, gestion des stocks, flux de vente, etc.),
- Les besoins de sécurité exprimés ou risques critiques.

Cette phase devait être réalisée à travers trois canaux d'acquisition d'informations en mode dégradé : des entretiens sur site avec différentes parties intéressées (direction, utilisateurs, responsables d'équipes…) pour 8 entreprises, des entretiens téléphoniques pour 8 entreprises et un questionnaire en ligne pour 40 entreprises.

Cyberdiag : mode d'acquisition de contexte.

► ***Ajustement***

Par manque d'entreprises candidates au début du projet cette phase d'acquisition de contexte spécifique au commerce est restituée dans le présent rapport Cyberdiag. Les spécificités du commerce et à la distribution en matière de cybersécurité ont été mises en lumière après les diagnostics et non avant comme cela avait été planifié.

2.1.2 Phase 2 : construction du diagnostic orienté Commerce et Distribution

Cette phase consiste en la conception du questionnaire du Cyberdiag au regard de l'acquisition de connaissances effectuée par l'intermédiaire des entretiens sur site, des entretiens par téléphone et par les questionnaires en ligne. Il s'agit de rédiger et d'établir un cadre méthodologique pour la réalisation du Cyberdiag. L'objectif étant de créer un cadre outillé permettant d'appliquer le diagnostic à toutes les entreprises participantes, dans les mêmes conditions.

Le Cyberdiag comporte 3 volets :

- Une auto-évaluation (Autodiag) qui donnera un score à l'entreprise,
- Des tutoriels qui permettent à l'entreprise d'appliquer un 1er niveau de sécurisation en auto-administration,
- Un diagnostic (basé sur un référentiel) permettant l'évaluation à un niveau plus fin d'analyse et de granularité.

Il est à noter qu'un dernier volet relatif à l'EDEC Commerce concerne l'expérimentation du Cyberdiag au travers de la remise d'un rapport relatant les enseignements de celle-ci.

► ***Ajustement***

Les difficultés de recrutement des entreprises et la temporalité rétrécie de l'expérimentation a modifié le projet de construction du référentiel du diagnostic. Cette partie de la phase 2 s'est avant tout reposée sur l'expérience de SCASSI en matière de conseil et d'audit en cybersécurité (plus de 80 actions par an).

2.1.2.1 L'Autodiag (auto-évaluation)

Avant la visite sur site de l'expert en cybersécurité, les entreprises participantes sont invitées à compléter l'Autodiag.

L'Autodiag est un questionnaire sécurité, disponible sur le site Internet du Cyberdiag-tpe-pme.com, dans l'espace personnel de l'entreprise. L'Autodiag permet au chef d'entreprise d'**évaluer le niveau de maturité initial** en matière de SSI de sa structure.

Ce questionnaire auto-administré a 2 objectifs principaux :

- permettre à l'entreprise de situer son niveau de maturité en SSI à travers un scoring en lettres, de A à E (E étant critique) et une appréciation,
- donner à l'expert en cybersécurité un premier niveau d'information en amont de sa visite sur site.

Le questionnaire, élaboré sur la base de l'expérience des experts en sécurité de SCASSI, permet aux entreprises de faire le point sur :

- le périmètre de leur SI (usages, outils informatiques, parc informatique et réseau),
- la prise en compte du risque dans leurs activités et les mesures de sécurité (physiques et informatiques) adoptées,
- l'organisation de la sécurité et les processus mis en œuvre.

L'Autodiag est articulé autour de **5 grandes thématiques** :

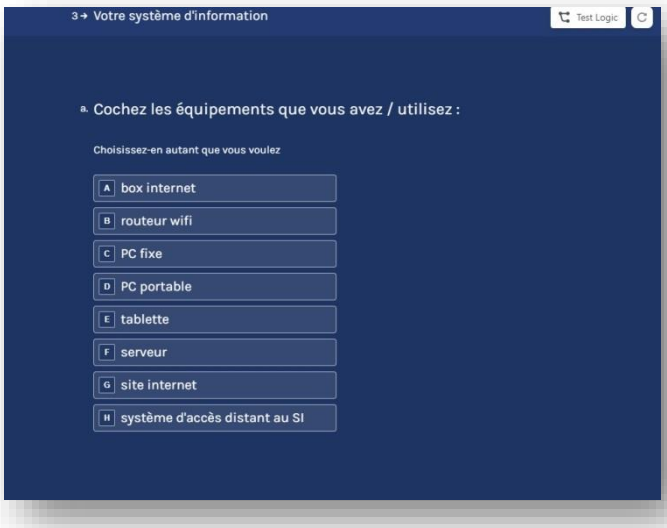
- les généralités,
- les locaux de l'entreprise,
- le système d'information,
- l'organisation de la sécurité,
- la sécurité des ressources humaines.

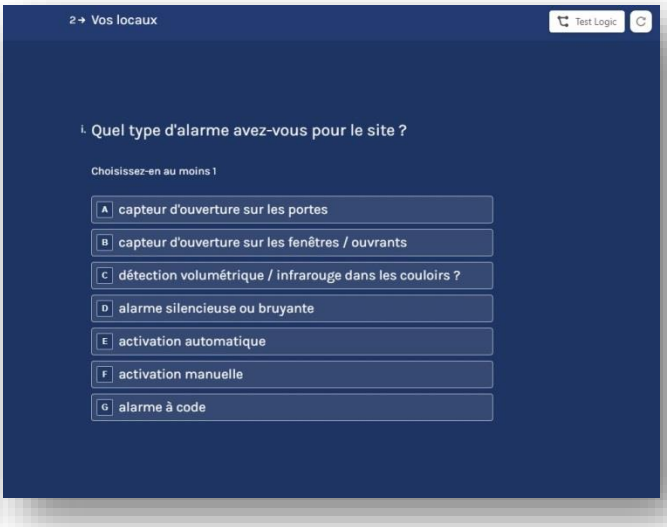
L'Autodiag contient 80 questions. La majorité des questions sont fermées avec des réponses à choix multiples qui sont analysées et donnent lieu à un score global s'affichant une fois le questionnaire terminé.

Les questions apparaissent à l'écran en fonction des réponses données et, de ce fait, ne sont pas toutes nécessairement proposées. Ainsi, un chef d'entreprise qui répondrait qu'il n'a pas de Firewall, ne verra pas de question demandant plus de détails à ce sujet (marque, nombre…).

Chaque entreprise a donc un chemin de questions différent et une durée de questionnaire variable estimée entre 20 et 35 minutes.

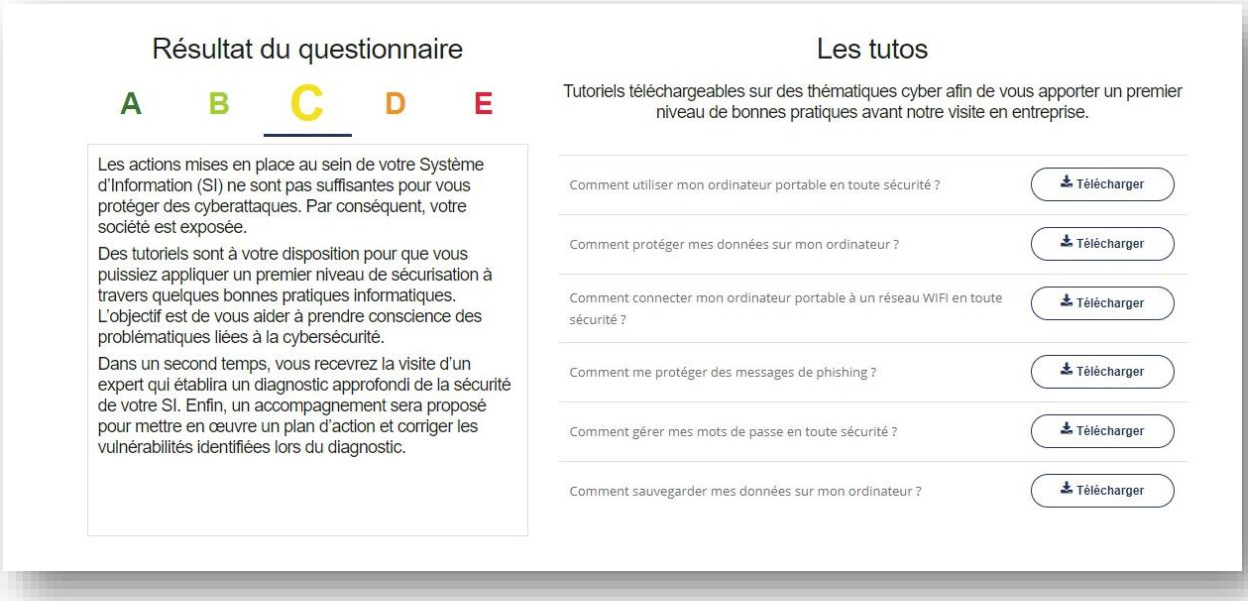
Autodiag – Exemples de questions posées





Une fois le questionnaire complété et terminé, **l'entreprise accède instantanément au résultat** du questionnaire et à des ressources cyber : les tutos.

Autodiag – Exemple de résultat (résultat et tutos)



2.1.2.2 Accès aux « tutos » (guides de bonnes pratiques)

Le résultat du questionnaire est corrélé à la mise à disposition de tutoriels (tutos/guides de bonnes pratiques).

L'objectif de ces 'tutos' est de répondre aux vulnérabilités les plus courantes des TPE/PME et de leur permettre une mise à niveau rapide de leur sécurité informatique. Ils représentent un premier pas vers la sécurisation du SI de l'entreprise à travers des bonnes pratiques à appliquer par les dirigeants et les collaborateurs. Les entreprises peuvent alors réagir avant même la visite sur site du consultant SCASSI.

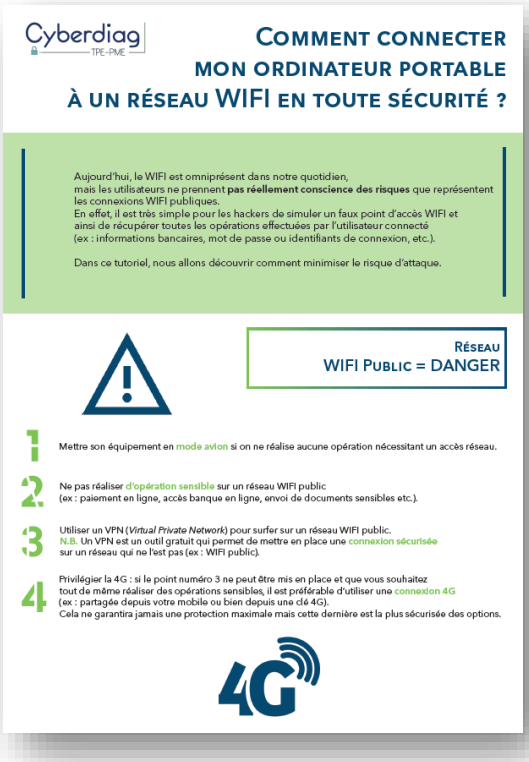
Ces guides pratiques, ont été créés par une équipe pluridisciplinaire composée d'experts en cybersécurité, de professionnels de la pédagogie et d'infographistes. Ils sont disponibles dans l'espace personnel de l'entreprise sous la forme de documents PDF recto/verso téléchargeables et imprimables.

L'approche de ces 'tutos' est résolument pragmatique. Ils ont été conçus pour être suivis 'pas à pas' avec des illustrations visuelles et peuvent être applicables immédiatement.

Les 6 'tutos' disponibles abordent les thèmes suivants :

- Bonnes pratiques avec un PC,
- Chiffrement,
- Connexion wifi,
- Détecter un email de phishing,
- Gérer ses mots de passe,
- Sauvegarde.

'Tuto' thématique 'Connexion Wifi'


Cyberdiag TPE-PME

COMMENT CONNECTER MON ORDINATEUR PORTABLE À UN RÉSEAU WIFI EN TOUTE SÉCURITÉ ?

Aujourd'hui, le WIFI est omniprésent dans notre quotidien, mais les utilisateurs ne prennent **pas réellement conscience des risques** que représentent les connexions WIFI publiques.
En effet, il est très simple pour les hackers de simuler un faux point d'accès WIFI et ainsi de récupérer toutes les opérations effectuées par l'utilisateur connecté (ex : informations bancaires, mot de passe ou identifiants de connexion, etc.).

Dans ce tutoriel, nous allons découvrir comment minimiser le risque d'attaque.

RÉSEAU WIFI PUBLIC = DANGER

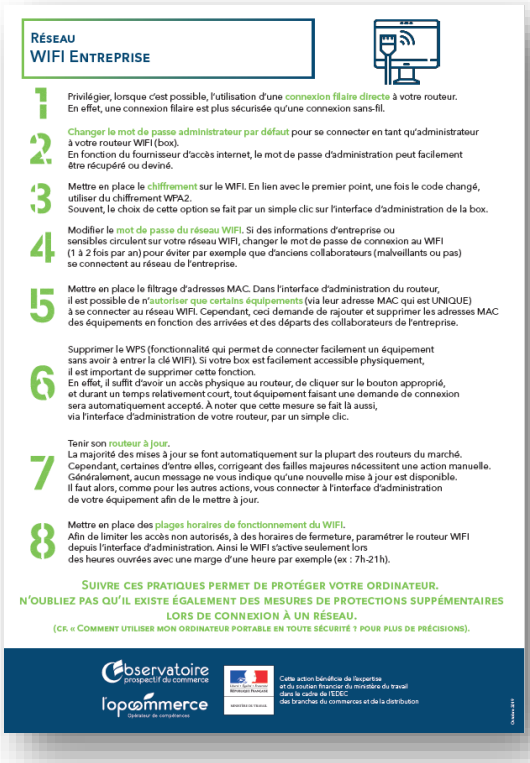
1 Mettre son équipement en mode avion si on ne réalise aucune opération nécessitant un accès réseau.

2 Ne pas réaliser d'opération sensible sur un réseau WIFI public (ex : paiement en ligne, accès banque en ligne, envoi de documents sensibles etc.).

3 Utiliser un VPN (*Virtual Private Network*) pour surfer sur un réseau WIFI public.
N.B. Un VPN est un outil gratuit qui permet de mettre en place une connexion sécurisée sur un réseau qui ne l'est pas (ex : WIFI public).

4 Privilégier la 4G : si le point numéro 3 ne peut être mis en place et que vous souhaitez tout de même réaliser des opérations sensibles, il est préférable d'utiliser une connexion 4G (ex : partagée depuis votre mobile ou bien depuis une clé 4G).
Cela ne garantira jamais une protection maximale mais cette dernière est la plus sécurisée des options.

4G


RÉSEAU WIFI ENTREPRISE

1 Privilégier, lorsque c'est possible, l'utilisation d'une connexion filaire directe à votre routeur.
En effet, une connexion filaire est plus sécurisée qu'une connexion sans-fil.

2 Changer le mot de passe administrateur par défaut pour se connecter en tant qu'administrateur à votre routeur WIFI (box).
En fonction du fournisseur d'accès internet, le mot de passe d'administration peut facilement être récupéré ou deviné.

3 Mettre en place le chiffrement sur le WIFI. En lien avec le premier point, une fois le code changé, utiliser du chiffrement WPA2.
Souvent, le choix de cette option se fait par un simple clic sur l'interface d'administration de la box.

4 Modifier le mot de passe du réseau WIFI. Si des informations d'entreprise ou sensibles circulent sur votre réseau WIFI, changer le mot de passe de connexion au WIFI (1 à 2 fois par an) pour éviter par exemple que d'anciens collaborateurs (malveillants ou pas) se connectent au réseau de l'entreprise.

5 Mettre en place le filtrage d'adresses MAC. Dans l'interface d'administration du routeur, il est possible de n'autoriser que certains équipements (via leur adresse MAC qui est UNIQUE) à se connecter au réseau WIFI. Cependant, ceci demande de rajouter et supprimer les adresses MAC des équipements en fonction des arrivées et des départs des collaborateurs de l'entreprise.

6 Supprimer le WPS (fonctionnalité qui permet de connecter facilement un équipement sans avoir à entrer la clé WIFI). Si votre box est facilement accessible physiquement, il est important de supprimer cette fonction.
En effet, il suffit d'avoir un accès physique au routeur, de cliquer sur le bouton approprié, et durant un temps relativement court, tout équipement faisant une demande de connexion sera automatiquement accepté. À noter que cette mesure se fait là aussi, via l'interface d'administration de votre routeur, par un simple clic.

7 Tenir son routeur à jour.
La majorité des mises à jour se font automatiquement sur la plupart des routeurs du marché. Cependant, certaines d'entre elles, corrigeant des failles majeures nécessitant une action manuelle. Généralement, aucun message ne vous indique qu'une nouvelle mise à jour est disponible. Il faut alors, comme pour les autres actions, vous connecter à l'interface d'administration de votre équipement afin de le mettre à jour.

8 Mettre en place des plages horaires de fonctionnement du WIFI.
Afin de limiter les accès non autorisés, à des horaires de fermeture, paramétrer le routeur WIFI depuis l'interface d'administration. Ainsi le WIFI s'active seulement lors des heures ouvrées avec une marge d'une heure par exemple (ex : 7h-21h).

SUIVRE CES PRATIQUES PERMET DE PROTÉGER VOTRE ORDINATEUR.
N'OUBLIEZ PAS QU'IL EXISTE ÉGALEMENT DES MESURES DE PROTECTIONS SUPPÉMENTAIRES LORS DE CONNEXION À UN RÉSEAU.
(CF. « COMMENT UTILISER MON ORDINATEUR PORTABLE EN TOUTE SÉCURITÉ ? POUR PLUS DE PRÉCISIONS).

Observatoire prospectif du commerce
lopcommerce
Cette action bénéficie de l'expertise et du soutien financier du ministère du travail dans le cadre de l'EDEC des branches du commerces et de la distribution

2.1.2.3 Le référentiel

Le référentiel est la trame de diagnostic unique suivie par le consultant lors de son rendez-vous en entreprise. Ce référentiel d'évaluation est construit sur la base des bonnes pratiques promues par l'ANSSI[6].

15 thématiques sont abordées pendant le diagnostic.

Pour chacune de ces thématiques, l'entreprise est évaluée sur les différentes mesures de sécurité mises en œuvre, qu'elles soient organisationnelles ou techniques. Une note est alors attribuée pour chaque thématique, correspondant à un niveau sous forme de note allant de 1 à 4.

Si aucune mesure de sécurité est mise en œuvre, alors la note attribuée à l'entreprise par rapport à la thématique traitée sera la **plus faible**.

Si certaines mesures de sécurité sont mises en œuvre mais ne sont pas appliquées à l'ensemble des personnels ou systèmes (pratiques homogènes), alors la note attribuée sera **moyenne**.

Enfin, la **note la plus haute** attribuée pour une thématique donnée signifie que des mesures de sécurité sont appliquées de manière uniforme et homogène et que ces mesures sont contrôlées et formalisées.

Ainsi, le niveau de maturité global de l'entreprise en matière de SSI se décline selon 3 niveaux : faible, moyen et satisfaisant. Naturellement, ce niveau est défini à partir de la moyenne des notes obtenues pour les 15 thématiques.

Les thématiques abordées pendant le diagnostic/audit, à travers le référentiel permettent d'analyser la capacité des entreprises à :

- Organiser la sécurité,
- Sensibiliser et former,
- Maîtriser ses prestataires informatiques,
- Connaître le système d'information,
- Authentifier et contrôler les accès,
- Sécuriser les postes,
- Sécuriser les serveurs,
- Sécuriser le réseau,

[6] *Guide des bonnes pratiques de l'informatique, 12 règles essentielles pour sécuriser vous équipements informatique – 01/2017 - ANSSI-CGPME ; Guide d'Hygiène informatique, Renforcer la sécurité de sons système d'information en 42 mesures – 01/2017 - ANSSI*

- Sécuriser les données,
- Sécuriser le développement des applications,
- Gérer le nomadisme,
- Sécuriser l'administration,
- Maintenir le système d'information à jour,
- Gérer la sécurité des locaux,
- Contrôler la sécurité.

Grâce à l'utilisation d'un référentiel unique de diagnostic/audit, des rapports uniformisés sur la forme peuvent être remis aux entreprises et des conclusions peuvent être tirées de cette expérimentation.

2.1.2.4 Le rapport du Cyberdiag

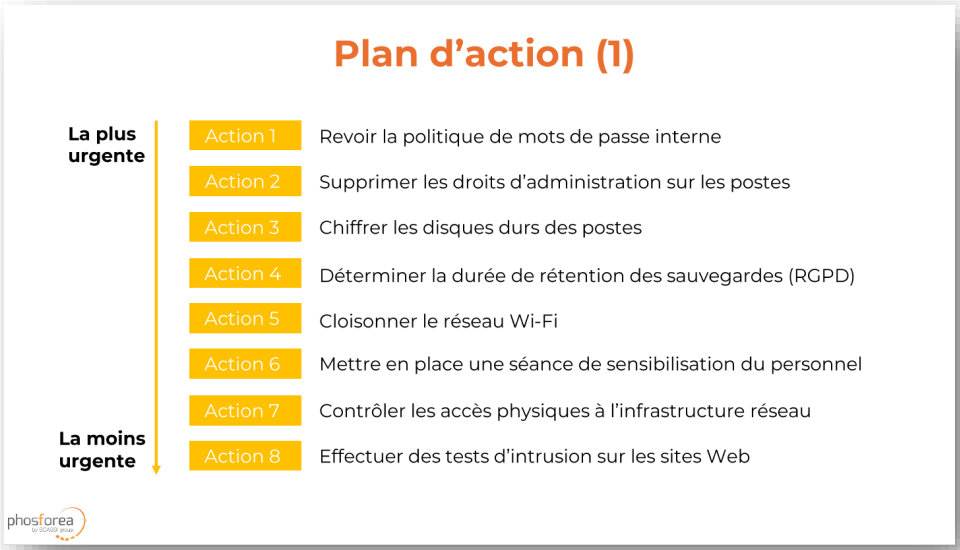
Suite à sa visite en entreprise, le consultant rédige **un rapport d'audit**, permettant de communiquer à l'entreprise diagnostiquée l'état des lieux de sa sécurité informatique actuelle ainsi que les recommandations d'actions à mener pour l'améliorer. L'approche du rapport se veut pédagogique et tend à vulgariser les termes techniques afin d'être compréhensible et appropriable par l'interlocuteur quel que soit son niveau d'expertise.

Un tableau est remis à l'entreprise analysant pour chacune des 15 thématiques évaluées, les constats faits sur site ainsi que des recommandations associées.

Cyberdiag : Rapport d'audit – Synthèse de l'évaluation

Le résultat du diagnostic/audit permet au consultant, en collaboration avec l'entreprise auditée, de définir un plan d'action (en tenant compte des problématiques de l'entreprise), pour mettre en œuvre les recommandations formulées par degré de criticité.

Cyberdiag : exemple de plan d'action préconisé à l'issue du diagnostic/audit



Enfin, **le consultant préconise des mesures d'accompagnement** en lien avec le plan d'action présenté. L'entreprise peut choisir de continuer à se faire accompagner dans le cadre du Cyberdiag ou d'arrêter la prestation dans la mesure où il a les compétences internes permettant la mise à niveau des préconisations.

Cyberdiag – Exemple de mesures d'accompagnement proposées

Mesure d'accompagnement	Charge (j)
Rédaction d'une charte informatique	0,5
Réalisation d'un processus de gestion des incidents	1,5
Réalisation d'une session de sensibilisation en présentiel à la sécurité informatique pour le personnel	0,5
Rédaction d'un document regroupant l'ensemble des exigences de sécurité à avoir dans les contrats avec ses prestataires	1,5
Mise en place de règles au sein du pare-feu	1,5

Le rapport d'audit, intégré dans un document Powerpoint (pour une meilleure lisibilité et un meilleur partage), est envoyé au contact entreprise via une procédure sécurisée (conteneur chiffré + code de déchiffrement transmis par un canal différent de l'envoi). Ces mesures de

sécurité sont en effet nécessaires car le rapport d'audit est une analyse poussée du SI et contient des données sensibles et confidentielles sur l'entreprise et ses failles potentielles.

2.1.3 Phase 3 : Test du diagnostic

Après la création du cadre outillé précédemment décrit, la troisième phase du projet porte sur l'expérimentation du Cyberdiag par les entreprises.

Pour se faire, il a été préconisé un découpage temporel en fonction de la taille des entreprises.

Cyberdiag : partie diagnostic/audit – préconisation selon la taille de l'entreprise

A cela s'ajoute l'accompagnement au choix de l'entreprise ainsi qu'un suivi téléphonique un mois après la fin de la prestation. L'objectif de ce suivi téléphonique est de relancer la dynamique cybersécurité au sein de l'entreprise, de recueillir les impressions à froid post-accompagnement en constatant la mise en œuvre ou pas du plan d'action.

2.1.3.1 La visite sur site (diagnostic physique)

La méthodologie et la démarche de diagnostic/audit sont celles adoptées par SCASSI et définies selon les spécifications de l'ISO 19011 : Norme internationale des lignes directrices pour l'audit des systèmes de management.

Suite à l'Autodiag, la visite sur site (diagnostic/audit en présentiel sur site de l'entreprise) a pris la forme d'entretiens entre le dirigeant de l'entreprise et/ou le salarié référent sur les thèmes de la sécurité et de l'informatique et le consultant en cybersécurité. Cette phase permet d'entrer dans un niveau de granularité SI plus fin à travers des échanges verbaux. L'évaluation est non seulement basée sur du déclaratif mais aussi sur des constats physiques dans les locaux. Par exemple :

- Des disques durs ou des clés USB contenant des informations sensibles non sécurisées,
- Des mots de passe à la vue de tous (affichage mural de codes wifi, mots de passe de de comptes sur des notes autocollantes, etc.),
- Des salles serveur en accès libre (sans local dédié ou porte non fermée),
- Des boitiers d'origine inconnue branchée sur le serveur,
- Des issues de secours non verrouillées.

En fin d'entretien, le consultant conclu par une restitution à chaud à l'oral. Cela permet immédiatement à l'entreprise de prendre conscience des vulnérabilités de son SI et éventuellement de parer au plus urgent dans l'attente de la remise du rapport.

2.1.3.2 L'accompagnement de l'entreprise dans la mise en œuvre de son plan d'action

L'option d'accompagnement a pour objectif de traiter les sujets prioritaires issus des recommandations et axes d'amélioration, tout en mettant à profit l'expérience et les compétences de SCASSI et Phosforea (expertise cybersécurité et pédagogie).

A cette étape du Cyberdiag, le consultant agit opérationnellement pour l'entreprise. Il met en œuvre son expertise pour appliquer effectivement les recommandations techniques pour l'entreprise.

L'entreprise bénéficiaire du Cyberdiag choisit à ce stade, si elle veut bénéficier de l'accompagnement, et alors elle détermine les actions que le prestataire exécutera pour et/ou avec elle, ou si elle est en capacité de mettre en œuvre le plan d'action avec ses ressources internes et donc de refuser l'accompagnement.

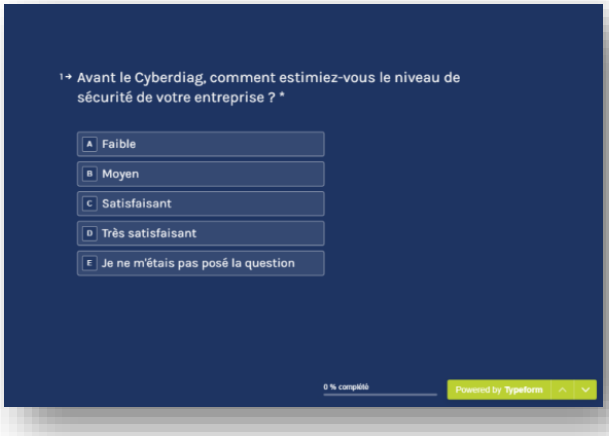
Exemples d'actions d'accompagnement réalisées par le prestataire

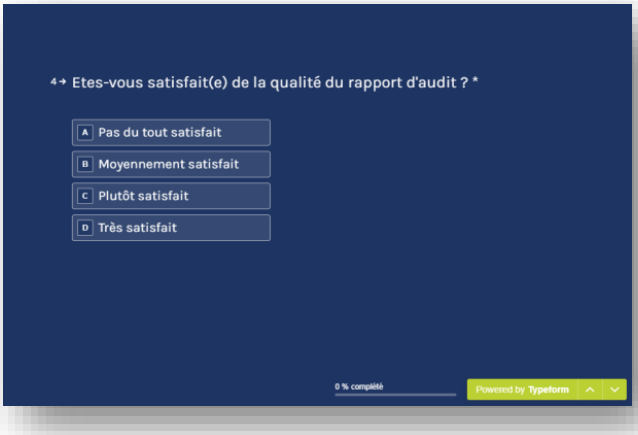
Documenter	Assister	Réaliser
• Politiques de sécurité • Chartes informatiques • Procédures de sécurité	• Coaching de proximité • Définir des priorités et des plans d'action • Appuyer la sensibilisation	• Tests d'intrusion • Scans de vulnérabilités • Revues de firewalls • Revues de droits

2.1.4 Phase 4 : Restitution

En fin d'expérimentation, un **questionnaire d'évaluation** est adressé aux entreprises ayant participé au Cyberdiag.

Questionnaire d'évaluation : exemple de questions





Ce questionnaire a pour but de recueillir les impressions des participants sur l'expérimentation. Celui-ci porte aussi bien sur la satisfaction globale des dirigeants ou des référents sécurité/informatique sur la prestation que sur leur perception de la cybersécurité.

La phase 4 constitue également l'objet du présent rapport. Elle permet de faire un retour sur l'ensemble des éléments relevés par Phosforea et SCASSI dans le cadre de l'expérimentation du Cyberdiag, d'en tirer des conclusions et d'effectuer des préconisations.

2.2 Parcours TPE/PME

Un des objectifs du Cyberdiag est de mobiliser le dirigeant de TPE/PME sur une durée la plus courte possible.

En effet, les dirigeants des entreprises de taille restreinte, et particulièrement celles du secteur du Commerce et de la Distribution, ont peu de disponibilités et sont souvent occupés par des tâches opérationnelles.

Ainsi, la durée moyenne de mobilisation envisagée, pour les interlocuteurs participants à l'expérimentation, est de 4 à 6 heures s'échelonnant sur 2 à 3 mois pour l'ensemble du processus.

Les TPE/PME prenant part au Cyberdiag expérimenteront un parcours client suivant les étapes listées ci-après.

Cyberdiag – Parcours TPE/PME

(Vue coté entreprise)

1. Rendez-vous téléphonique initial
2. Signature d'une convention d'audit, autorisation préalable à toute intervention dans l'entreprise
3. Réalisation en autonomie de l'Autodiag en ligne
4. Consultation des tutos
5. Visite sur site (diagnostic/audit)
6. Réception du rapport d'audit rédigé par le consultant
7. Restitution téléphonique
8. Choix des sujets sur lesquels l'entreprise souhaite un accompagnement approfondi
9. Execution de l'accompagnement par le prestataire (selon le choix de l'entreprise)
10. Rendez-vous téléphonique de suivi à 1 mois
11. Questionnaire d'évaluation
12. Signature de la feuille d'émargement

3. Experimentation du Cyberdiag

3.1 Recrutement des entreprises

Dans le cadre du projet, chaque branche impliquée devait être équitablement représentée en nombre et en tailles d'entreprises. Le COTECH a donc décidé que chacune des 8 branches, devait proposer 7 entreprises participantes soit un total de 56 entreprises pour l'opération.

S'agissant d'une action à coût zéro pour l'entreprise, c'est-à-dire prise en charge intégralement par l'Etat et l'Opcommerce, il était envisagé de nombreux candidats. Cependant l'expérimentation a été confrontée à plusieurs contraintes et obstacles :

- Le **très haut niveau de charge de travail supporté par les dirigeants** des TPE/PME du commerce, pour qui la gratuité de l'accompagnement est un élément attrayant mais manifestement insuffisant à leur permettre de participer ;
- La **sur-sollicitation des TPE/PME** pour divers types d'actions imposant de faire des choix et de prioriser leurs actions ;
- La **méconnaissance de la sécurité informatique** pour laquelle les TPE/PME n'ont pas toujours d'appétence et beaucoup appréhension, orientant au mieux le sujet vers leur prestataire ;
- La **période de lancement de l'opération** en avril 2019 qui, par manque d'entreprises candidates a été repoussée en juin sur la période de solde, puis en juillet période estivale puis septembre 2019 avec un nombre restreint d'entreprises malgré un démarchage soutenu.

Bien que le COTECH ait demandé un triptyque sur lequel s'appuyer, expliquant simplement et succinctement l'expérimentation Cyberdiag, l'univers de la sécurité informatique est difficile à appréhender et à expliquer notamment à cause d'un vocabulaire spécifique qui mérite d'être vulgarisé.

Les difficultés précédemment décrites ont, à plusieurs reprises, eu pour effet de décaler le projet dans le temps, faute d'un nombre suffisant d'entreprises participantes.

Il est à noter que **les branches professionnelles** étaient par ailleurs déjà sollicitées sur d'autres expérimentations de l'EDEC Commerce et de ce fait, au total, ce sont **10 entreprises** qui ont été proposées par les branches pour le Cyberdiag :

- 1 entreprise de 50/299 pour l'import-export,
- 4 pour l'Optique-lunetterie de détail (3 moins de 11 salariés et 1 de 11/49 salariés),
- 5 pour le Commerce de détail et de gros à Prédominance alimentaire (1 de 11/49 salariés, 3 de 11/49 salariés, 1 de 50/299 salariés).

En conséquence de ces difficultés de recrutement d'entreprises, la phase d'acquisition de contexte décrite en 2.1 n'a pu être exécutée en amont du projet et, pour éviter de mettre en péril le reste du projet, cette phase a été décalée pendant la phase de diagnostic/audit sur site. L'expérimentation a pu être lancée fin septembre 2019 soit 3 mois avant la fin de réalisation de l'action dans le cadre de l'EDEC Commerce.

Les difficultés rencontrées par les branches pour recruter des entreprises a invité le COTECH, en juin 2019, à transférer la sélection d'entreprises à l'Opcommerce. Ainsi, l'Opcommerce a organisé une campagne d'appels sortants sur une cible d'entreprises adhérentes des 8 branches impliquées. Cette phase a été réalisée de juin à août 2019.

Afin de limiter les frais annexes (transport/hébergement), c'est la délégation Occitanie de **l'Opcommerce** qui a été pressentie comme région test (région pouvant s'emparer du projet, prestataire sur la région limitant les frais). Plus de 200 appels sortants ont été émis par les collaborateurs de l'Opcommerce région Occitanie pendant la période estivale. Bien que cette période soit peu propice aux contacts avec les entreprises, un nombre significatif d'entreprises se sont inscrites à l'expérimentation : **18 entreprises**.

Les autres délégations régionales de l'Opcommerce ont été sollicitées mais l'offre de service n'a pas retenu l'attention des entreprises.

Avant la fin 2019, sur le **site dédié www.cyberdiag-tpe-pme.com ce sont 6 entreprises** qui ont postulé au Cyberdiag (1 entreprises de moins de 11 salariés pour la branche du commerce à distance et 5 entreprises de l'import-export : 3 de 11/49 salariés et 2 de 50/299 salariés).

Phosforea a pu identifier à travers son réseau, **1 entreprise** de moins de 11 salariés répondant aux critères d'éligibilité de la branche Optique-lunetterie de détail.

Début octobre 2019, l'Opcommerce a lancé un emailing à destination des entreprises de 5 à 250 salariés des branches impliquées dans l'expérimentation. Cet emailing a été ciblé sur les régions Ile-de-France et Nouvelle Aquitaine, sans résultat.

Synthèse de 35 entreprises intéressées par le Cyberdiag	
ENTREE BRANCHE PROFESSIONNELLE	**10**
Import-Export	**1**
50/299	1
Optique-lunetterie de détail	**4**
-11	3
11/49	1
Commerce à prédominance alimentaire	**5**
11/49	4
50/299	1
ENTREE PRESTATAIRE	**1**
Optique-lunetterie de détail	**1**
-11	1
ENTREE SITE INTERNET	**6**
Commerce à distance	**1**
-11	1
Import-Export	**5**
11/49	3
50/299	2
ENTREE L'OPCOMMERCE	**18**
Commerce à distance	**9**
-11	4
11/49	3
50/299	2
Succursaliste de la chaussure	**1**
-11	1
Horlogerie-bijouterie de détail	**1**
-11	1
Import-Export	**5**
-11	2
11/49	3
Photographe	**1**
11/49	1
Commerce à prédominance alimentaire	**1**
-11	1
Total	**35**

Il est à noter que suite à leur accord de principe initial, plusieurs entreprises sont finalement sorties du projet. Les raisons de ces désistements sont de plusieurs ordres :

- 2 entreprises dont le SI était géré en Europe (Pays-Bas et Royaume Unis) :
    - Import-Export : 1 moins de 11 salariés et 1 de 50/299 salariés.
- 4 entreprises intéressées mais n'ayant pas répondu dans les temps :
    - Import-Export : 2 de 11/49 salariés et 2 de 50/299 salariés.
- 2 entreprises entrées par la branche mais n'ayant ni répondu aux mails ni aux appels téléphoniques :
    - Commerce à prédominance alimentaire : 2 de 11/49 salariés
- 1 entreprise dont le dirigeant était souffrant :
    - Optique-lunetterie de détail : moins de 11 salariés.

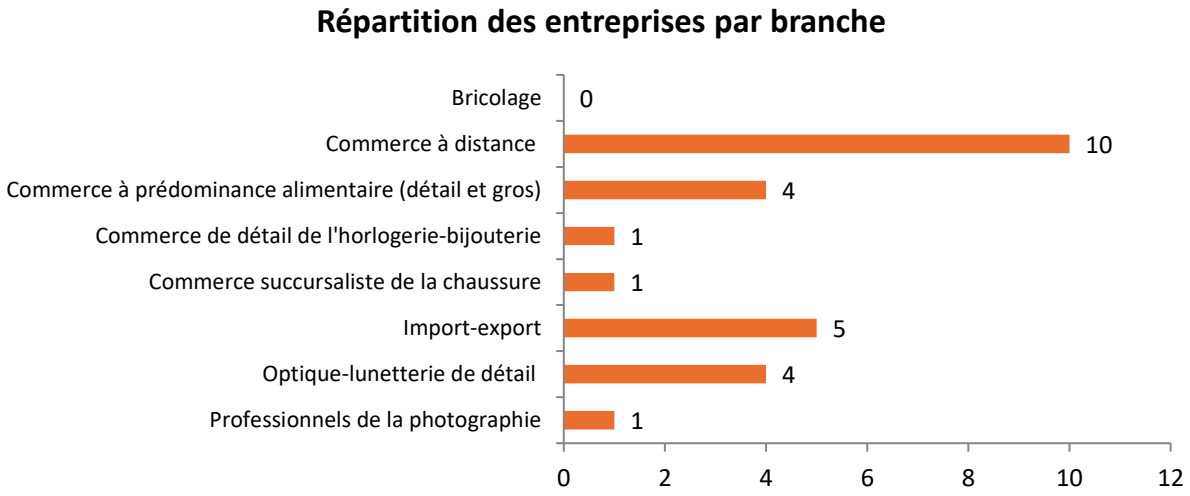
Synthèse de 26 entreprises entrées dans le Cyberdiag	
VALIDE BRANCHE PROFESSIONNELLE	**6**
Optique-lunetterie de détail -11 11/49	**3** 2 1
Commerce à prédominance alimentaire 11/49 50/299	**3** 2 1
VALIDE PRESTATAIRE	**1**
Optique-lunetterie de détail -11	**1** 1
VALIDE SITE INTERNET	**2**
Commerce à distance -11	**1** 1
Import-Export 11/49	**1** 1
VALIDE L'OPCOMMERCE	**17**
Commerce à distance -11 11/49 50/299	**9** 4 3 2
Succursaliste de la chaussure -11	**1** 1
Horlogerie-bijouterie de détail -11	**1** 1

Import-Export -11 11/49	**4** 1 3
Photographe 11/49	**1** 1
Commerce à prédominance alimentaire -11	**1** 1
Total	**26**

⇨ **Sur un prévisionnel initial de 56 entreprises, ce sont finalement 26 entreprises qui ont été expérimentatrices du Cyberdiag, soit 46% du prévisionnel.**

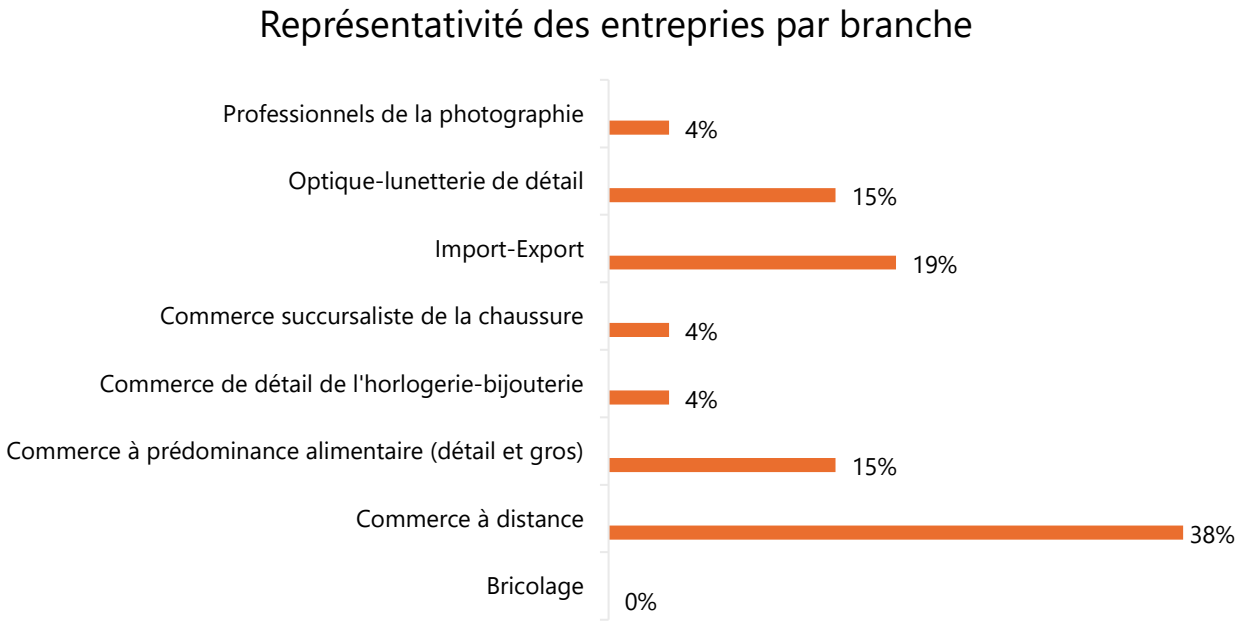
3.1.1 Répartition des entreprises par branche

A l'arrêt du recrutement des entreprises, ce sont 26 entreprises qui ont intégré l'expérimentation Cyberdiag.



Au total, ce sont 7 branches qui ont été représentées sur les 8 impliquées dans l'expérimentation. Les entreprises de la branche du Bricolage, bien que contactées téléphoniquement, ont décliné l'offre dans la mesure où elles sont souvent rattachées à un groupe et n'ont pas d'autonomie sur leur SI.

Il convient de souligner que toutes les branches ne sont pas représentées à parts égales.



Les branches du Commerce à distance et de l'import-export représentent à elles deux plus de la moitié (57%) des entreprises expérimentant le Cyberdiag.

Les branches de l'Optique lunetterie de détail et de la Prédominance alimentaire représentent quant à elles 30% des entreprises. Les 12% restants étant répartis à parts égales entre l'Horlogerie bijouterie de détail, les Professionnels de la photographie et le Commerce succursaliste de la chaussure.

Comme proposé initialement, un minimum de 7 entreprises était requis pour pouvoir distinguer les tendances propres à un secteur d'activité. Au vu des entreprises impliquées, hors-mis pour le Commerce à distance, il est peu pertinent et possiblement dangereux de faire des focus spécifiques par secteur d'activité.

Eclairage quant au nombre d'entreprises par branche :

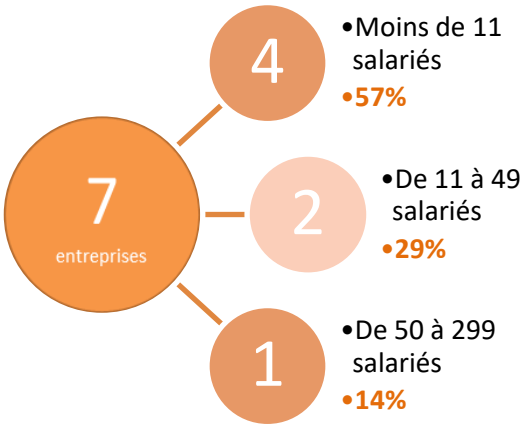
- **Commerce à distance** : Initialement 10 entreprises intéressées et **10 entreprises recrutées** sur 7 dans la démarche. Ce secteur utilisateur d'outils informatiques, de l'Internet, des réseaux sociaux… est en appétence pour l'informatique et ses outils, et a accueilli le projet avec enthousiasme ;
- **Import-Export** : Initialement 11 entreprises intéressées mais **5 entreprises recrutées** sur 7 dans la démarche. Deux entreprises se sont retirées du projet dans la mesure où leur SI était piloté et géré dans d'autres pays Européens, 4 entreprises d'un groupe qui n'a pas répondu dans les temps malgré des échanges très soutenus. A relever un intérêt certain partagé par l'ensemble des entreprises ;

- **Commerce à prédominance alimentaire (détail et gros)** : Initialement 6 entreprises intéressées et **4 entreprises recrutées** sur 7 dans la démarche. Malgré le soutien de la branche et de leur enseigne, 2 n'ont pas donné suite ni aux messages téléphoniques ni aux mails transmis. Un secteur dont le SI est souvent verrouillé par les groupes et qui manque de temps pour se consacrer au sujet.
- **Optique-lunetterie de détail :** Initialement 5 entreprises intéressées et **4 entreprises recrutées** sur 7 dans la démarche. Une entreprise s'est désistée du projet dans la mesure où son dirigeant était souffrant.
- **Horlogerie-bijouterie de détail** : Initialement 1 entreprise intéressée et **1 entreprise recrutée** sur 7 dans la démarche. Un secteur difficile d'accès, une méfiance ressentie lors des échanges téléphoniques pouvant être lié au fait que ce secteur a particulièrement été éprouvé par de nombreuses attaques physiques pouvant expliquer la méfiance des interlocuteurs.
- **Professionnels de la photographie** : Initialement 1 entreprise intéressée et **1 entreprise recrutée** sur 7 dans la démarche. Un secteur se disant pas intéressé par la démarche.
- **Commerce succursaliste de la chaussure** : Initialement 1 entreprise intéressée et **1 entreprise recrutée** sur 7 dans la démarche. Un secteur qui informe ne pas avoir de temps pour s'y consacrer avec un intérêt limité sur le sujet voire qui n'a pas Internet. Un refus en lien avec un précédent démarchage effectué par Agefos Pme Occitanie sur le même sujet ayant apporté une confusion dans l'esprit de l'entreprise qui refusera finalement le Cyberdiag.
- **Bricolage** : Initialement 0 entreprises intéressées sur 7 prévues dans la démarche. Pour un certain nombre, elles font partie d'un groupe qui gère le SI. Beaucoup de refus par manque d'intérêt pour la proposition ou par manque de temps pour s'y consacrer.

3.1.2 Répartition des entreprises par taille

Initialement la répartition des entreprises par branche professionnelle devait se faire par tranche d'effectif.

Schéma prévisionnel de la répartition des entreprises par branche

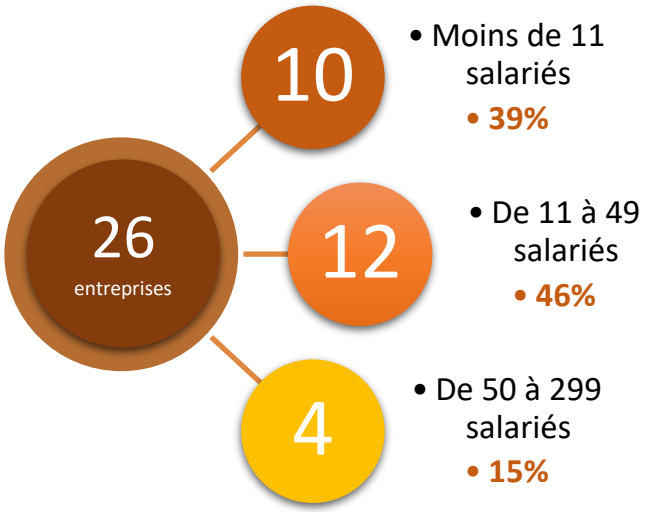


Au vu de ce schéma, l'objectif était de favoriser l'accompagnement des entreprises inférieures à 50 salariés dans la sécurisation de leur SI. Elles représentaient 86% des entreprises.

Face aux difficultés de recrutement, ce prévisionnel visant à sélectionner des entreprises a été assoupli. Pour favoriser l'expérimentation, la sélection des entreprises par tranche d'effectif a été assouplie et le plafond de 7 entreprises par branche a été supprimé.

Ainsi, le profil des entreprises accompagnées lors de l'expérimentation a varié selon les branches professionnelles.

Répartition des entreprises ayant expérimenté le Cyberdiag par tranche d'effectif



A la réalisation il est constaté que les entreprises de moins de 50 salariés, qui sont au nombre de 22, représentent 85% des entreprises participantes, contre un prévisionnel de 86%.

Le détail de la répartition entre les entreprises de moins de 11 salariés représentant 38% contre 57% initialement prévu, et les entreprises de 11 à 49 salariés représentant 46% contre 29%, montre une plus grande difficulté à convaincre les TPE à s'engager dans la démarche.

⇨ **L'objectif de favoriser les entreprises de moins de 50 salariés a été atteint.**

3.1.3 Une expérimentation à l'échelle nationale

Afin de limiter l'impact des coûts liés aux déplacements et hébergements le cas échéant, la prospection téléphonique menée par l'Opcommerce s'est concentrée particulièrement (mais pas uniquement) sur la zone sud-ouest du territoire national où est installé le siège de Phosforea en Haute-Garonne. Décision validée par le COTECH n° 5 du 27 mai 2019.

Le panel d'entreprises est réparti sur l'ensemble du territoire national comme suit :

- 15 entreprises sont installées en région Occitanie dont 9 en Haute-Garonne,
- 3 entreprises sont en Grand-Est,
- 3 entreprises sont en Ile-de-France,
- 2 entreprises sont en Centre-Val de Loire,
- 1 entreprise est en Bretagne,
- 1 entreprise est en Normandie,
- 1 entreprise est en Nouvelle Aquitaine.

3.2 Rendez-vous et Autodiag

3.2.1 Prise de rendez-vous

Une fois les entreprises participantes identifiées par les Branches professionnelles et l'Opcommerce, le premier contact avec Phosforea a consisté en un entretien téléphonique. Cet entretien avait un triple objectif :

- Prise de contact et présentation des parties prenantes,
- Explication détaillée de la démarche et réponses aux questions (objectif/enjeux),
- Prise de rendez-vous pour la réalisation du diagnostic/audit sur site.

Cette phase du projet a été particulièrement chronophage et sous-estimée en amont malgré l'identification préalable effectuée par les branches et l'Opcommerce.

En effet, la disponibilité des interlocuteurs en entreprises étant très aléatoire. En moyenne, il a été nécessaire de réaliser 2 à 3 séances de phoning avant de parvenir à joindre le bon interlocuteur pour fixer un rendez-vous.

Après cet entretien téléphonique permettant de valider l'entrée de l'entreprise dans la démarche du Cyberdiag, une confirmation du rendez-vous par mail a été systématiquement envoyée à l'interlocuteur ainsi qu'un email d'activation lui permettant d'accéder à son espace personnel et effectuer l'Autodiag en ligne, soit 2 emails.

Malgré ces précautions apportées à de la phase de prise de rendez-vous, 2 audits ont dû être replanifiés et ont généré des frais :

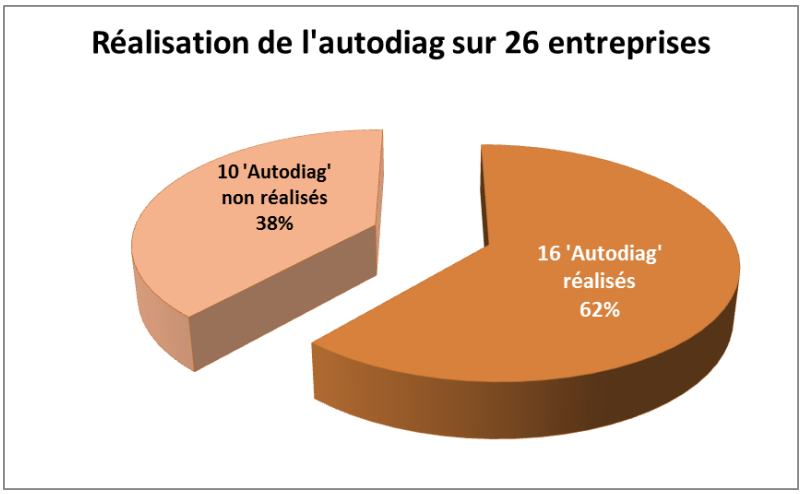
- Un problème d'adresse : l'adresse du listing ne correspondait pas à l'adresse du lieu de rendez-vous (ces adresses étant distantes de plus de 250 km ;
- Un problème d'agenda : le client n'avait pas noté le rendez-vous et était indisponible à l'heure convenue.

3.2.2 Réponses à l'Autodiag

Pour contextualisation, avant la visite sur site de l'expert en cybersécurité (auditeur), les entreprises participantes sont invitées à compléter l'Autodiag qui est un questionnaire sécurité, disponible sur le site Internet www.Cyberdiag-tpe-pme.com dans l'espace personnel de l'entreprise. Après

L'Autodiag permet au chef d'entreprise d'évaluer le niveau de maturité SSI initial de sa structure et permet à l'expert en cybersécurité un premier niveau d'information en amont de sa visite sur site.

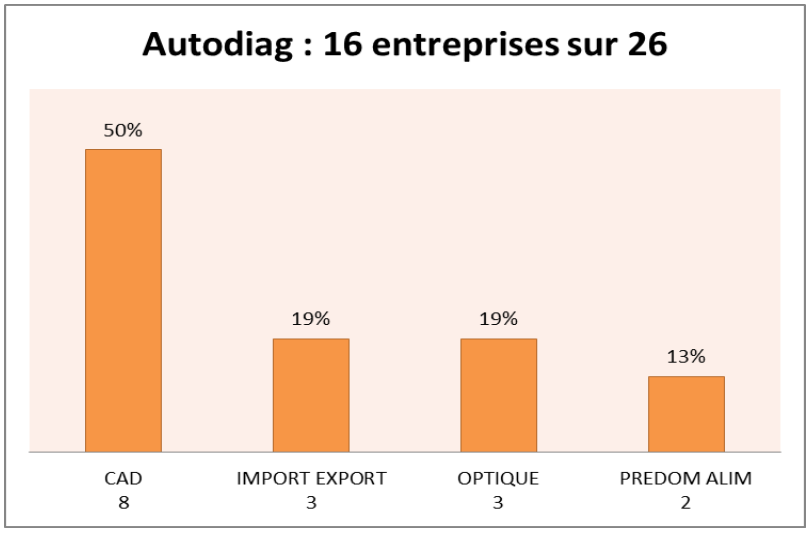
La complétude ou non de l'Autodiag laisse un indice sur l'implication de l'entreprise dans la démarche. Sur 26 entreprises, seules 16 ont pris le temps de répondre au questionnaire en ligne.



Les visuels ci-dessus indiquent que **plus de la moitié des entreprises ont complété l'Autodiag**. Cependant, pour atteindre ce résultat, de nombreuses relances téléphoniques et mails ont été nécessaires.

En effet, l'Autodiag couvrant tout le périmètre du SI, le nombre de questions posées parait relativement conséquent. Pourtant, lorsque l'entreprise prend le temps d'y répondre, elle appréhende généralement mieux le périmètre couvert par l'expérimentation Cyberdiag et se sent préparée aux différentes questions qui surviendront lors de l'entretien sur site.

De plus, ce questionnaire préliminaire à la visite sur site, permet à l'auditeur de se faire une 1ère idée du contexte de l'entreprise ainsi que des mesures de sécurité mises en œuvre au sein du SI. L'auditeur dispose alors d'informations lui permettant d'alimenter sa réflexion et d'orienter certaines de ses questions lors de l'entretien sur site.



Les entreprises de la branche du Commerce à distance sont plus promptes à effectuer l'Autodiag.

⇨ **L'Autodiag permet, lorsqu'il est réalisé en amont par l'entreprise, de gagner du temps lors de la visite sur site et d'obtenir des informations plus pertinentes.**

3.3 Visites sur site

3.3.1 Un grand intérêt lors des visites sur site

La visite sur site du consultant cybersécurité est sans aucun doute l'étape de l'expérimentation Cyberdiag qui a suscité le plus grand intérêt de la part des entreprises.

En effet, la présence d'un consultant sur site représente une opportunité d'échanger sur des problématiques de cybersécurité qui peuvent parfois paraître complexes pour les entreprises. Le consultant constitue alors une interface privilégiée pour rassurer et informer les dirigeants et personnes en charge des fonctions de sécurité (RSSI, responsable informatique…).

La visite sur site peut être assimilée à la première étape d'un accompagnement sur-mesure de l'entreprise car le consultant est à l'écoute de son interlocuteur. Les premières minutes de dialogue sont alors décisives pour le convaincre de l'importance de la cybersécurité pour l'entreprise.

De plus, un des enjeux majeurs de cette visite sur site est de faire en sorte que l'interlocuteur comprenne que **les objectifs de l'entreprise en matière SSI peuvent s'aligner avec ses objectifs stratégiques.**

L'accueil du consultant par l'entreprise varie d'une entité à l'autre.

En effet, il est vrai que les personnes interviewées sont souvent des dirigeants, PDG ou DAF et par leur fonction, disposent de très peu de temps à consacrer au consultant. Ainsi, l'interview sur site est souvent ponctué d'interruptions plus ou moins espacées. **L'efficacité de cet entretien dépend de l'intérêt de la personne interviewée pour la prestation, et de sa capacité à rester concentrée**.

Un autre facteur différenciant pour que la visite sur site soit pertinente concerne les informations que possède l'interlocuteur. Ainsi, deux entretiens ont duré uniquement une heure à cause du manque d'informations de la personne interviewée (branche Optique-Lunetterie de détail). La conséquence de ce type d'entretien est qu'il conduit à un rapport incomplet puisque l'auditeur n'a pas été en mesure de récolter toutes les informations nécessaires.

Par ailleurs, l'expérimentation Cyberdiag a permis de constater différentes approches et différentes conditions d'accueil lors de la venue du consultant sur site.

En effet, si une majorité de dirigeants/responsables sont enthousiastes et se réjouissent de la venue du consultant, d'autres sont plus réservés quant à la plus-value de cette rencontre. Mais pour la plupart d'entre eux, la cybersécurité reste un vaste concept qui leur semble parfois lointain et complexe et la visite sur site leur a donné l'opportunité de comprendre les enjeux cybersécurité actuels.

A noter que pour 2 dirigeants (branches Horlogerie-bijouterie de détail et Optique-lunetterie de détail), il a fallu réexpliquer les basiques de l'informatique avant de pouvoir intégrer toutes les problématiques inhérentes au concept de cybersécurité. 2 dirigeants/responsables (branches Optique-lunetterie de détail et Commerce à prédominance alimentaire) ont cependant douté de l'intérêt de la venue sur site du consultant. Souvent, cette réaction était due au fait qu'ils n'étaient pas convaincus des risques qui pesaient sur le SI de l'entreprise.

Sur 26 audits réalisés, deux se sont déroulés dans des conditions particulières.

Dans le 1er cas (branche commerce de détail de l'horlogerie-bijouterie de moins de 11 salariés), le dirigeant était seul sur son point de vente, aussi, il lui a été difficile d'assurer le rendez-vous en plus de l'accueil des clients.

Dans le 2nd cas (branche Optique-lunetterie de détail de 11 à 49 salariés) l'interlocuteur a été remplacé au pied levé par un salarié qui n'avait aucune connaissance du SI. Cela a donné lieu à un entretien écourté par le manque de matière à récolter.

Dans le cas de ces deux entreprises, la prise de contact téléphonique a été révélatrice du peu d'intérêt que présentaient les dirigeants à l'égard de l'expérimentation Cyberdiag et le la cybersécurité en général.

La plus-value de la visite sur site réside surtout dans l'écoute de l'auditeur et au fait qu'il illustre ses propos de ses nombreuses expériences ou de faits qu'il a pu constater tout au long de ses missions : c'est ce qui le légitimise auprès des entreprises. Une majorité d'entreprises ont pu s'identifier à des exemples cités par l'expert, ce qui leur a permis de se projeter pour aborder au mieux les enjeux de cybersécurité.

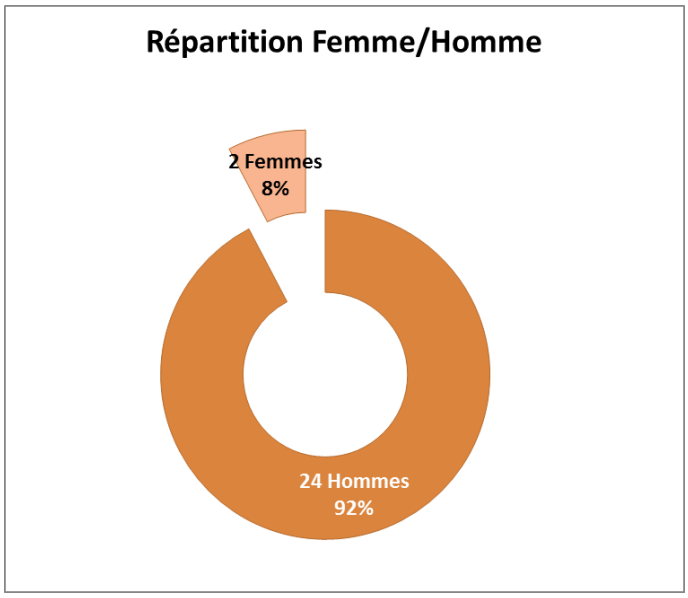
En conclusion, l**a visite sur site constitue une phase centrale dans l'expérimentation Cyberdiag** puisqu'elle permet :

- Une première sensibilisation des parties prenantes à la cybersécurité,
- Une restitution/analyse orale « à chaud » des constats faits sur site et du niveau global de maturité SSI de l'entreprise.

Ainsi, la Direction de l'entreprise peut disposer d'un 1er avis sans attendre la restitution du rapport. Le regard du consultant extérieur à l'entreprise (certifié ANSSI, porté par l'Opcommerce) est particulièrement écouté et apprécié car il se veut impartial.

3.3.2 Parité

L'expérimentation Cyberdiag a permis de constater la faible part de femmes dans la sécurité des SI et notamment au sein des TPE/PME. **Sur les 26 entreprises auditées, seules 8% des femmes occupent un poste en lien avec la sécurité du SSI.**



Cette statistique issue du projet Cyberdiag est à rapprocher des travaux de l'éditeur de logiciel Kaspersky Lab[7] qui montrent qu'il n'y a que 11% de femmes dans la cybersécurité. L'article insiste sur le fait que cette tendance se retrouve également chez les jeunes : 78% des adolescentes interrogées n'ont jamais envisagé une carrière dans ce domaine.

C'est d'ailleurs ce qu'explique Nacira SALVAN, présidente du CEFCYS (CErcle des Femmes de la CYberSécurité), dans un article[8] dédié à la promotion de cette association loi 1901 créée en 2016, qui a pour objet de promouvoir la parité femme-homme dans un milieu historiquement très masculin.

3.4 Restitution téléphonique et plan d'action

La restitution téléphonique a 3 objectifs dans le projet :

- Présenter aux TPE/PME les conclusions de l'audit de manière détaillée et illustrée au travers d'un rapport,
- Répondre aux éventuelles questions,
- Présenter les recommandations d'actions et co-construire le plan d'action.

---

[7] Source : Global Security Mag, Article de Kaspersky Mag, Mars 2019, 'Femmes et carrière en cybersécurité : les raisons d'un désamour' : https://www.globalsecuritymag.fr/Femmes-et-carriere-en,20190306,85105.html

[8] Source : Le Monde Informatique : Interview Nacira Salvan, Présidente du CEFCYS : 'Le rôle des femmes en cybersécurité est nécessaire et insuffisant' : https://www.lemondeinformatique.fr/actualites/lire-interview-nacira-salvan-presidente-du-cefcys--le-role-des-femmes-en-cybersecurite-est-necessaire-et-insuffisant-77998.html

Il est important de préciser que certaines restitutions ont dû être décalées en raison de l'indisponibilité du client et ce, bien que la date de restitution ait été fixée d'un commun accord au préalable.

Focus sur les 26 entreprises participantes au Cyberdiag :

- **18 entreprises** ont bénéficié de la restitution téléphonique ;
- **4 entreprises** (3 de la branche Commerce à distance et 1 de l'Import-Export) ont mis en place des actions préconisées par le consultant durant la restitution à chaud, sans attendre l'envoi du rapport et la restitution téléphonique. Cela démontre une réelle proactivité de ces entreprises à l'issue de l'audit/diagnostic sur site, et du pragmatisme du plan d'actions préconisé ;
- **4 entreprises** n'ont pas bénéficié de cette restitution téléphonique pour les raisons suivantes :
    - 3 entreprises (branches commerce à prédominance alimentaire, Optique-lunetterie de détail et Horlogerie-bijouterie de détail de moins de 11 salariés) n'ont pu libérer du temps pour la réunion téléphonique malgré de multiples rappels et reports du rendez-vous. La visite sur site leur semblait suffisante et leur avait permis d'avoir un premier niveau d'information à travers la restitution à chaud. Cela veut aussi dire qu'ils étaient satisfaits de cette prestation sur site,
    - 1 entreprise (branche commerce à prédominance alimentaire de 11 à 49 salariés) a avancé des difficultés techniques à l'ouverture du rapport (malgré les diverses aides techniques apportées par le chef de projet, et n'a pas souhaité donner suite).

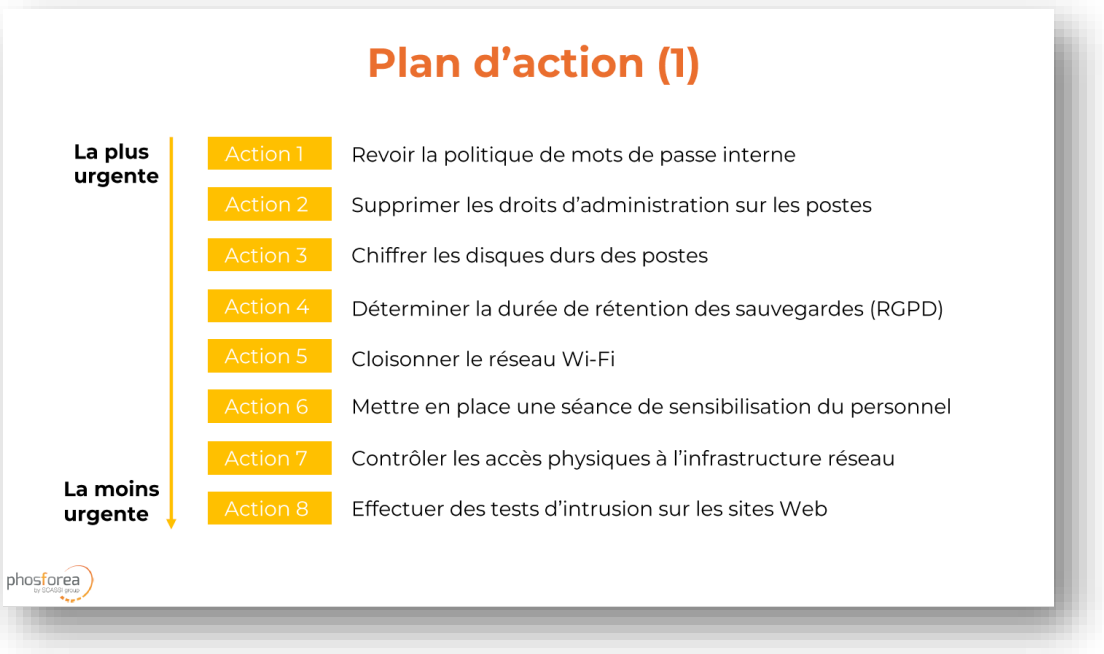
Le rapport d'audit/diagnostic fourni pas le consultant, outre l'état des lieux de la sécurité de l'entreprise, **met en lumière des actions à mener, classées par ordre de priorité** afin d'augmenter le niveau de sécurité de l'entreprise. L'objectif est que l'entreprise comprenne pour chaque ligne les enjeux et l'attention à y porter.

Pour les entreprises l'ayant consulté, il a été unanimement qualifié de clair et précis. Des participants de la branche Optique-lunetterie de détail ont fait part de leur intention d'en faire la promotion au sein de leur réseau.

A cette étape de restitution**, le prestataire et l'entreprise co-construisent un plan d'action** sur la base des préconisations de l'expert. L'entreprise a alors le choix de les réorganiser par priorité ou capacité d'application. Ces actions peuvent être échelonnées dans le temps sauf si des vulnérabilités majeures sont constatées.

⇨ **Toutes les restitutions réalisées ont permis de mettre en avant la satisfaction des clients quant à la qualité de la prestation sur site ainsi que celle du rapport, pour les clients qui en ont pris connaissance.**

Exemple de plan d'action



En fin de rendez-vous téléphonique, au regard du plan d'action préconisé, voire réorganisé par l'entreprise, celle-ci a 2 options :

- **Continuer le Cyberdiag avec l'accompagnement renforcé** :
  - Sélection de plusieurs items d'accompagnement.
- **D'arrêter là le Cyberdiag :**
  - Mise en place des recommandations avec ses ressources internes.

Dans l'expérimentation, **8 entreprises n'ont pas souhaité bénéficier de l'accompagnement renforcé** :

- 1 entreprise (Commerce à distance) avait les ressources internes pour mettre le plan d'action validé à la restitution téléphonique du rapport ;
- 3 entreprises (Commerce à prédominance alimentaire, Horlogerie-bijouterie de détail, Optique-lunetterie de détail) ont lu le rapport mais n'ont pas assisté à la restitution téléphonique et n'ont pas donné suite ;
- 4 entreprises (1 de la branche Commerce à distance, 3 de la branche Commerce à prédominance alimentaire) se sont inscrites à l'expérimentation du Cyberdiag

tardivement et le temps disponible en fin de projet était trop court pour mettre en place un accompagnement.

3.5 Accompagnement renforcé

L'accompagnement renforcé est une partie optionnelle du Cyberdiag dont l'objectif est de traiter les sujets prioritaires issus des préconisations faites par le consultant. A cette étape du Cyberdiag, le consultant agit opérationnellement pour l'entreprise pour appliquer les recommandations techniques pour l'entreprise.

L'accompagnement renforcé a été retenu par 69% des entreprises (18 sur 26).

Au total, les consultants experts en cybersécurité ont réalisé **72 jours d'accompagnement pour 18 entreprises.** Cela représente **une moyenne de 4 jours d'accompagnement par entreprise**.

Les accompagnements les plus demandés par les entreprises ont été la rédaction personnalisée de documents (les entreprises pouvant choisir plusieurs prestations) :

- Exigences de sécurité dans les contrats prestataires (67% des entreprises),
- Processus de gestion des arrivées, mouvements et départs des salariés (56% des entreprises),
- Charte informatique (56% des entreprises).

Pour répondre à ces besoins, Phosforea a créé à plusieurs documents qui s'adressent directement aux TPE/PME :

- Gestion des arrivées, mouvements et départs des collaborateurs ;
- Exigences de sécurité dans les contrats prestataires ;
- Charte informatique ;
- Gestion des incidents de sécurité ;
- Politique de Sécurité du Système d'Information (PSSI) ;
- Tutoriels d'installation/configuration de logiciels.

Les équipes de consultants en sécurité ont apporté la plus grande attention à la rédaction de ces documents en prenant en compte la réalité 'terrain' des TPE/PME. Ce sont des supports pragmatiques, sur mesure et contextualisés. Ces livrables didactiques, ont été rédigés en employant un vocabulaire accessible afin d'être directement applicables sur le terrain.

En effet, la rédaction de ces documents peut s'avérer relativement chronophage lorsqu'elle est réalisée par une personne non initiée. L'intervention des consultants en sécurité a donc

permis un gain de temps non négligeable à l'entreprise ainsi que la garantie de qualité et de conformité des documents.

En plus de la rédaction de ces documents, les entreprises ont sollicité les accompagnements suivants :

- Sensibilisation à la cybersécurité en présentiel (11%) ;
- Prospection de prestataires informatiques (5%) ;
- Mise en place de règles au sein du pare-feu (firewall) (5%) ;
- Test d'intrusion sur site web (11%).

Dans le souci de produire des livrables bénéficiant aux entreprises en mobilisant un minimum les dirigeants, Phosforea a optimisé les échanges qui se sont fait majoritairement par email. Cette démarche a été très appréciée par les participants.

Le plébiscite de l'accompagnement documentaire **démontre le besoin de formaliser la sécurité au sein des TPE/PME**. Des bonnes pratiques ne suffisent pas, il est également nécessaire de formaliser toutes les actions mises en place.

La sensibilisation/formation SSI en présentiel a quant à elle été particulièrement appréciée par les 2 entreprises (branches Professionnels de la photographie et Commerce à distance de 11 à 49 salariés) qui en ont fait la demande.

En effet, elle a suscité l'attention des collaborateurs qui y ont assisté et se sont prêtés au jeu de questions/réponses sur une demi-journée. Après la séance de sensibilisation/formation, les collaborateurs ont échangé sur leurs pratiques informatiques, parfois à risque. Cela a permis au dirigeant de prendre conscience que certains comportements liés à l'usage des ressources du SI allaient à l'encontre de la stratégie de sécurité de l'entreprise.

3.6 Relance à 1 mois

Afin de mesurer l'impact de l'expérimentation Cyberdiag et la capacité des entreprises à s'investir sur le sujet de la cybersécurité, les équipes de Phosforea ont assuré un suivi téléphonique 1 mois près la fin de la prestation. **L'objectif étant de 'faire une piqûre de rappel cybersécurité' à l'entreprise et de voir si elle a commencé à mettre en œuvre son plan d'action.**

Ce suivi téléphonique « à froid » a permis de faire ressortir les points suivants :

- Les dirigeants de TPE/PME ont un niveau d'occupation très élevé et ne parviennent pas, malgré la prise de conscience provoquée par le Cyberdiag, à dégager du temps pour mettre en place le plan d'action ;

- La mise en œuvre des recommandations suppose la disponibilité de trésorerie ou de temps humain : débloquer le budget correspondant peut s'avérer compliqué, tout comme mobiliser les compétences qui ne seraient alors plus attelées à la production courante ;
- Le délai d'un mois leur semble trop court. La mise en œuvre de pratiques de sécurisation du SI d'une TPE/PME doit se programmer sur un temps plus conséquent (plusieurs mois). Ce n'est pas un chantier qui est à exécuter exclusivement à court-terme.

Il convient préciser que les entreprises ayant choisi d'être accompagnées pour le déploiement du plan d'action ont bénéficié d'un **suivi régulier de la part de Phosforea**. En effet, lors de la phase d'accompagnement, les interactions entre le consultant et l'entreprise sont réguliers, aussi bien pour récolter des informations permettant de mener à bien la mission que lors de la restitution des documents produits ou de l'éventuelle intervention sur site. Les constats listés précédemment lors du suivi « à froid » avaient donc souvent été listés avant l'appel téléphonique.

3.7 Evaluation

Dans le but d'évaluer le niveau de satisfaction des entreprises participantes, le prestataire a envoyé à l'ensemble des entreprises un questionnaire d'évaluation en ligne, à la fin du projet. Ce questionnaire se compose des 9 questions suivantes assorties de 4 réponses au choix :

1. Avant le Cyberdiag, comment estimiez-vous le niveau de sécurité de votre entreprise ?
2. Ce diagnostic vous a-t-il permis de prendre conscience de l'importance de la cybersécurité pour votre organisation ?
3. Etes-vous satisfait(e) de la qualité de l'intervention de l'auditeur sur site ?
4. Etes-vous satisfait(e) de la qualité du rapport d'audit ?
5. Est-ce que les conclusions du rapport d'audit vous ont permis de choisir votre accompagnement de façon éclairée ?
6. Si vous avez choisi des mesures d'accompagnement, êtes-vous satisfait(e) de la qualité des prestations / livrables ?
7. Recommanderiez-vous le Cyberdiag à une entreprise du commerce ?
8. Avez-vous des commentaires sur le Cyberdiag ?
9. Auriez-vous effectué le Cyberdiag s'il n'avait pas été intégralement pris en charge par l'Etat et l'Opcommerce ?

10 entreprises sur les 26 participantes, ont répondu aux 9 questions posées en ligne.

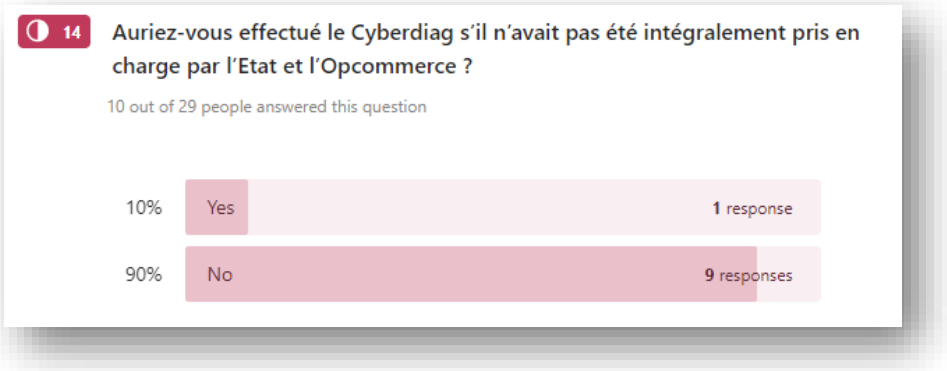
Entreprises ayant répondu à l'évaluation	
Commerce à distance -11 11/49 50/299	**6** 2 3 1
Optique-Lunetterie de détail -11	**1** 1
Import-Export -11	**1** 1
Photographe 11/49	**1** 1
Commerce à prédominance alimentaire 11/49	**1** 1
Total	**10**

L'analyse de ces évaluations permet de faire ressortir les informations marquantes suivantes :

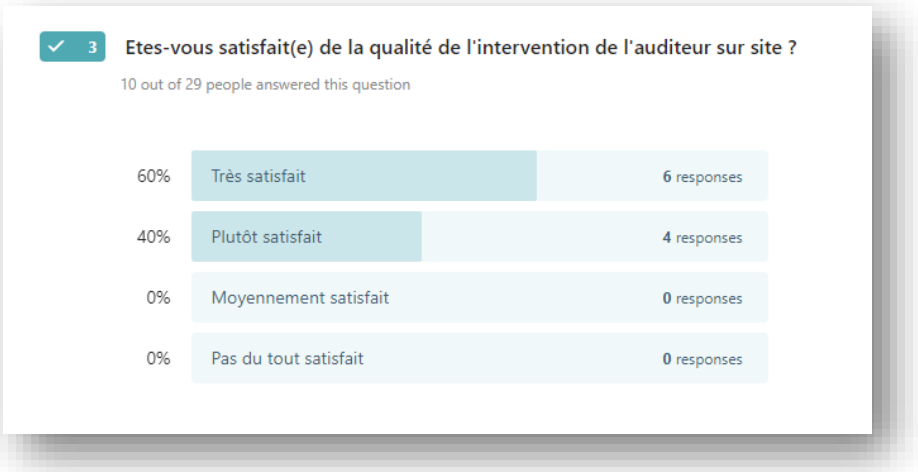
- En amont du Cyberdiag :
  - 40% des entreprises estimaient leur niveau de sécurité « faible » ou « moyen ».
  - 60% le pensaient « satisfaisant » ou « très satisfaisant ».
- 40% des répondants affirment que le dispositif Cyberdiag leur a permis de prendre conscience des risques cyber.

Le Cyberdiag dans ses modalités actuelles est largement plébiscité par les participants : à la question ***« Recommanderiez-vous le Cyberdiag à une entreprise du commerce »***, 100 % ont répondu « OUI ».

Le critère financier reste prédominant pour les TPE/PME : 9 entreprises sur 10 affirment que le caractère entièrement gratuit de l'action Cyberdiag a été déterminant dans leur adhésion au dispositif.



D'un point de vue purement qualitatif, 100% des répondants jugent l'intervention de l'auditeur sur site et la qualité du rapport d'audit « satisfaisant » à « très satisfaisant ».



3.8 Le Cyberdiag en quelques chiffres

4. SYNTHESE ET PRECONISATIONS

4.1 Une empreinte commerce ?

Les entreprises du commerce et plus particulièrement celles qui disposent de points de vente et/ou disposent de stocks dans leurs locaux, sont **sensibilisées aux problématiques de sécurité physique**. La majorité de ces entreprises a mis en œuvre une sécurité périmétrique et volumétrique élevée au sein de ses locaux : capteurs de détection de mouvements, contrôle d'accès à l'entrée de l'entreprise, caméras de vidéosurveillance, surveillance par un vigile, etc., représentent autant de moyens auxquels ces entreprises ont recours. Ces entreprises, pour la télésurveillance/vidéosurveillance de leurs locaux, font généralement appel à des prestataires extérieurs.

En matière de sécurité, les entreprises du commerce investissent dans des mesures de sécurité physiques qui s'avèrent parfois très onéreuses ; Pour autant, elles sont souvent plus frileuses à allouer un budget à la SSI. Pourquoi ?

Une hypothèse pour répondre à cette interrogation est que les produits commercialisés au sein de ces entreprises, représentent une valeur marchande significative parce que matériellement identifiables. Ainsi, le vol à l'étalage de produits (lunettes, bijoux, denrées alimentaires, etc.) est une action concrète dont il est aisé d'évaluer les répercussions financières de façon quasi immédiate. Or, pour ces entreprises (qui commercialisent des produits matériellement identifiables), il est beaucoup plus compliqué d'évaluer les répercussions financières d'une cyberattaque qui n'est pas toujours identifiable de par son immatérialité. Tant que l'entreprise n'est pas attaquée, elle n'est pas consciente de la matérialité d'une attaque (blocage des ordinateurs, défiguration de pages web…).

Pourtant, à ce jour, les cyberattaques sont si développées que leurs impacts peuvent être considérables pouvant aller jusqu'à causer la fermeture de l'entreprise. Par exemple, les attaques de type « ***cryptolocker*** » (logiciel malveillant qui vise à verrouiller l'ordinateur en vue d'un rançonnage) sont si évoluées qu'elles sont capables de chiffrer les disques durs de tous les postes de travail et serveurs d'un SI, y compris les équipements de sauvegarde (Ex. les NAS : Network Attached Storage = Stockage en réseau), s'ils sont connectés à ce SI. Si l'entreprise ne dispose pas de sauvegarde externalisée ou que les dispositifs de sauvegarde ne sont pas déconnectés du SI, elle peut tout perdre en quelques minutes. Rares sont celles qui arrivent à refaire surface lorsqu'elles ont perdu tout l'historique de leur facturation, base de données client, fiches produits, comptabilité… Ainsi, une cyberattaque peut avoir des conséquences bien plus dévastatrices que le vol à l'étalage… Malheureusement toutes les entreprises du commerce n'en sont pas encore conscientes.

Ainsi, l'enjeu majeur aujourd'hui est de communiquer auprès des dirigeants de ces petites structures pour qu'ils puissent considérer la cybersécurité comme une priorité, malgré le peu de temps dont ils disposent. Cependant, même si le dirigeant de l'entreprise prend conscience des enjeux cybersécurité et souhaite mettre en place des mesures de sécurité, l'allocation d'un budget propre à ce besoin est indispensable. Ce budget permettrait alors à l'entreprise de financer des prestations externalisées auprès de professionnels qualifiés, de mettre en place des actions de sensibilisation et de formation pour ses collaborateurs souhaitant porter des fonctions de sécurité ou intégrer au SI des matériels et des logiciels de sécurité. Toutes ces mesures techniques et organisationnelles contribueront à rendre les TPE/PME moins vulnérables face aux attaques actuelles et nouvelles à venir.

Enfin, d'un point de vue cybersécurité, l'analyse des entrants (données récoltées au cours de l'expérimentation) ne relève pas d'une empreinte spécifique au commerce et à la distribution. **Les usages, pratiques et risques, sont plutôt assimilés à une empreinte TPE/PME liés à la taille de l'entreprise.** Cet éclairage repose sur le croisement de l'expérimentation Cyberdiag avec l'expérience de SCASSI et Phosforea sur les audits et accompagnement des entreprises de tailles similaires.

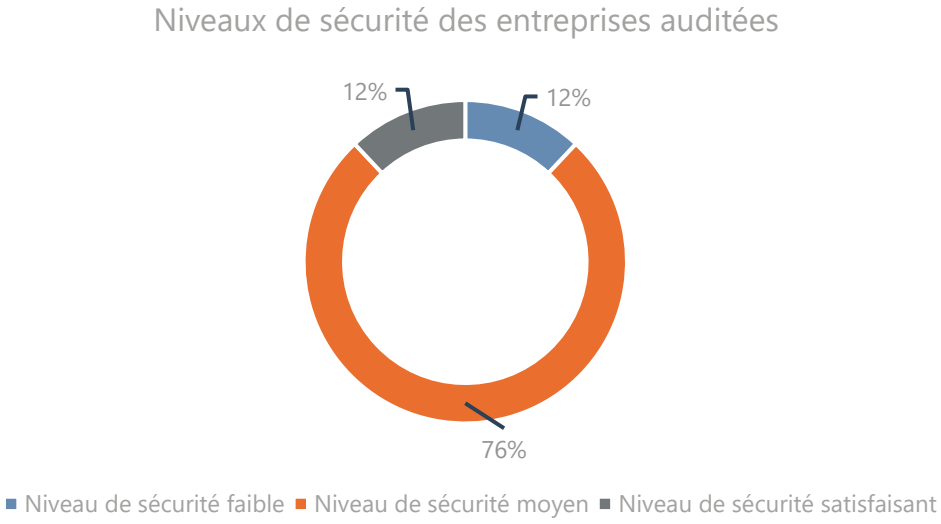
Les vulnérabilités les plus communément rencontrées dont il est question dans la suite de ce document, sont partagées par toutes les branches. **Ces vulnérabilités sont le reflet de la maturité des TPE/PME en matière de SSI**. En effet, pour la plupart, ces vulnérabilités peuvent être corrigées sans un effort trop conséquent et ne demandent pas d'investissement ni même de compétences spécifiques (exemple : changement de la politique de mots de passe interne). En conclusion, ce qu'il manque aux TPE/PME, c'est le temps requis pour mettre en place des mesures de sécurité de manière uniforme et surtout une prise de conscience des risques.

4.2 Evaluation de la maturité SSI des TPE/PME du commerce et de la distribution

Comme cela a été indiqué précédemment, la maturité des entreprises a été évaluée sur site, selon un référentiel couvrant une quinzaine de thématiques de cybersécurité ;

L'expérimentation Cyberdiag a révélé que :

- 12% des entreprises auditées ont un niveau de sécurité faible,
- 76% ont un niveau de sécurité moyen,
- 12% possèdent un niveau de sécurité satisfaisant.



4.2.1 Les points forts communs aux entreprises participantes

- **Une surface d'attaque restreinte due au faible nombre d'équipements informatiques :**

L'expérimentation Cyberdiag a permis de constater que la taille du parc informatique est proportionnelle au nombre de collaborateurs. En effet, **comme le nombre d'équipements présents au sein du parc est souvent réduit, la probabilité qu'une personne externe malveillante exploite une vulnérabilité sur l'un de ces équipements est plus faible**. De plus, l'utilisation de ces équipements est relativement basique (consultation d'emails, de pages Web, connexion à l'ERP et à des espaces collaboratifs, etc.). Il convient de souligner que peu d'entreprises laissent la possibilité à leurs collaborateurs de se connecter au SI à distance, à l'exception du dirigeant. Là encore, cela contribue à diminuer les risques d'infection.

- **Une tendance à déléguer l'infogérance du parc informatique à un tiers professionnel qualifié :**

L'expérimentation Cyberdiag a permis de constater que **50% des TPE/PME externalisent l'infogérance de leur parc informatique.** Cette délégation permet de garantir un certain niveau de sécurité et de réactivité en cas d'incident. Toutefois, toutes les entreprises ne sont pas égales quant à la protection de leur SI puisque certains prestataires intègrent de manière inégale les problématiques de cybersécurité au sein du périmètre de leurs prestations.

- **La présence d'un référent cybersécurité**

Il a été constaté que la présence d'une personne ayant une appétence pour la cybersécurité au sein de l'entreprise impacte directement le niveau de maturité de celle-ci en matière de SSI. En effet, comme cette personne communique sur les différentes problématiques de cybersécurité à l'ensemble des employés, les mauvaises pratiques informatiques sont généralement moins fréquentes.

4.2.2 Les principales vulnérabilités constatées

4.2.2.1 Un sentiment d'absence d'exposition aux risques

L'expérimentation Cyberdiag a révélé que la prise en compte des enjeux de cybersécurité par les entreprises était inégale et dépendait pour beaucoup du secteur d'activité de l'entreprise et du nombre de ses collaborateurs.

En effet, **une minorité de TPE/PME pensent encore ne pas être concernées par les cyberattaques au vu du faible nombre de collaborateurs qu'elles emploient.** Or, dans le contexte actuel, même si ces dernières ne sont pas ciblées de façon intentionnelle, elles n'en restent pas moins vulnérables aux cyberattaques de masse (exemple : cryptolocker, phishing, etc.).

L'outil informatique, bien que présent dans toutes les branches, répond à un besoin différent d'une entité à l'autre. Il occupe une place plus ou moins importante selon l'activité de l'entreprise. À titre d'exemple, les entreprises de la branche *Commerce à distance* sont beaucoup plus dépendantes du bon fonctionnement de leur système d'information (exemple : serveurs), du fait que les ventes par Internet soient au centre de leur activité.

De plus, le contexte (concurrentiel, environnemental...) varie d'une entreprise à l'autre ; **toutes ne sont pas confrontées aux mêmes enjeux de cybersécurité.**

4.2.2.2 Entreprises conscientes du besoin de disponibilité du SI et de l'intégrité des données

Globalement, les entreprises qui ont conscience des enjeux cybersécurité auxquels elles sont confrontées, sont aussi celles qui sont capables d'identifier les scénarii de risque, c'est-à-dire la vraisemblance qu'une menace (hacker, concurrent...) exploite une vulnérabilité sur un actif (site Web, logiciels, réseaux, etc.) présent au sein du SI de l'entreprise.

Les entreprises les plus matures savent mesurer l'impact de ces scénarii de risque qui sont étroitement liés au contexte du SI. Elles sont donc capables de mettre en œuvre des mesures de sécurité qui traitent les risques (réduction du risque, évitement, transfert, résilience, etc.) et permettent de limiter les impacts d'une attaque sur le SI.

L'enjeu de sécurité, par rapport à un actif (constituant une valeur pour l'entreprise), se mesure souvent selon quatre critères :

- *Disponibilité* : la probabilité qu'une donnée soit accessible et opérationnelle à un instant donné ;
- *Intégrité* : garantir que les données qui sont accédées ne sont pas altérées ;
- *Confidentialité* : assurer que seules les personnes autorisées accèdent aux données ;
- *Preuve ou traçabilité* : conserver des traces des opérations effectuées sur les données et les protéger pour qu'elles constituent des preuves, notamment en cas d'incident de sécurité.

En résumé, les entreprises mettent en œuvre des mesures de sécurité techniques ou organisationnelles en fonction d'un besoin de sécurité sur un actif. Par exemple, **les entreprises de la branche du Commerce à distance, ont un réel besoin de sécurité quant à leur site Web (actif transactionnel) qui occupe une place centrale dans la stratégie de l'entreprise**. En effet, si le site Internet de ce type d'entreprise devient indisponible de façon momentanée ou prolongée, cela a des répercussions financières immédiates, qui sont plus ou moins conséquentes puisque que les clients ne sont plus en mesure d'acheter des produits. Un scénario de risque peut être l'exploitation d'une faille du site Web par un hacker le rendant indisponible grâce à une attaque par déni de service (attaque visant à rendre indisponible le service).

En revanche, pour les entreprises de la branche **Optique-lunetterie de détail**, le besoin de sécurité est porté sur les **données de santé relatives aux clients** et par conséquent sur les supports (serveur, poste de travail, logiciel, etc.) qui font transiter ces informations. Ainsi, en cas de divulgation de ces données de santé sur un réseau public, l'impact sera juridique (cf. RGPD) et l'image de l'entreprise pourra en être considérablement affectée. La conséquence finale de cette réaction en chaine pourra être **une perte financière significative liée à la perte de confiance de la clientèle.**

Enfin, la prise en compte des enjeux de cybersécurité et des besoins de sécurité des entreprises dépend de la perception de chacune d'entre elles. En effet, toutes ne sont pas conscientes des risques qui pèsent sur leur SI, ni même des impacts que pourraient engendrer certaines attaques. Par ailleurs, toutes ne sont pas égales quant à leur capacité à maintenir leur activité en cas d'incident de sécurité. Tous ces éléments conditionnent directement la maturité des entreprises en matière de SSI.

Parmi les 26 entreprises auditées dans le cadre de l'expérimentation Cyberdiag, plusieurs vulnérabilités sont récurrentes quelle que soit la taille de l'entreprise ou quelle que soit sa branche.

4.2.2.3 Les vulnérabilités techniques communes aux TPE/PME

Les vulnérabilités techniques présentées ci-dessous sont classées par « fréquence de constat » au cours des 26 audits réalisés :

- **L'absence de politique de mots de passe robustes**

La vulnérabilité majeure la plus retrouvée durant les audits est : la politique de mots de passe interne de l'entreprise.

Pour une majorité d'entreprises, **aucune politique de mots de passe n'a été définie** et les mots de passe utilisés sont rarement renouvelés. Par conséquent, cela se traduit par la liberté, pour les collaborateurs, de construire leurs mots de passe comme bon leur semble. Le risque est l'utilisation de mots de passe faibles composés de mots du dictionnaire avec peu de caractères et étant parfois fortement corrélés au nom de l'entreprise. Ces mots de passe sont également réutilisés sur plusieurs applications.

Dans d'autres cas, des **mots de passe par défaut** sont communiqués par le référent sécurité ou l'administration réseau aux collaborateurs. Néanmoins, la majorité du temps, ces derniers ne prennent pas le temps de modifier ces mots de passe souvent trop simples.

Enfin, il a été constaté que des référents sécurité ou administrateurs systèmes et réseaux définissaient des mots de passe pour les comptes Windows ou de messagerie les utilisateurs. De cette façon**, ils sont en possession des mots de passe de tous les utilisateurs** et peuvent utiliser leur compte lorsque cela leur semble nécessaire, ce qui représente un risque d'usurpation l'identité numérique des utilisateurs. Le risque de perte ou de vol en masse de ces données constitue également un risque non négligeable qui pourrait avoir des conséquences graves en cas de diffusion publique.

- **Le défaut de configuration des postes de travail et des droits d'administration**

La seconde vulnérabilité la plus constatée concerne la configuration des postes. En effet, dans la majorité des cas, **des données sensibles sont stockées sur les disques durs internes des postes mais celles-ci ne sont pas chiffrées** (le chiffrement permet de rendre illisible les données aux personnes ne possédant pas la clé de déchiffrement que seul l'utilisateur est sensé connaitre). Cela est d'autant plus dangereux pour le personnel nomade (dirigeants, commerciaux) qui est amené à se déplacer et à fréquenter des lieux publics (Wifi public représentant souvent une opportunité de piratage des données).

De plus, au sein des TPE/PME, les utilisateurs travaillent, pour la plupart, à partir d'un **compte d'administrateur local de leur poste**. Ce type de compte confère les plus hauts privilèges sur un poste. En cas d'attaque (Exemple du Phishing : clic sur une pièce jointe piégée), sa portée sera d'autant plus dévastatrice étant donné que toutes les actions sont autorisées

depuis ce compte. Il est donc important d'utiliser ce type de compte avec parcimonie, pour réaliser uniquement des opérations d'administration.

- **Un besoin de sensibilisation aux problématiques de cybersécurité**

Les collaborateurs des entreprises sont très peu sensibilisés aux problématiques de cybersécurité et plus particulièrement aux attaques les plus répandues. Les attaques de type phishing sont néanmoins celles auxquelles les collaborateurs sont le plus sensibilisés.

Il y a un **réel besoin de sensibilisation/formation à la cybersécurité dans les TPE/PME**. Plusieurs modalités existent : e-learning, conférence, formation présentielle… La sensibilisation en présentiel qui a pu être dispensée dans deux entreprises participantes au Cyberdiag, dans le cadre de l'accompagnement approfondi, a été reçue très positivement par les salariés. Ce type de sensibilisation interactive retient l'attention des salariés et leur fait prendre conscience plus efficacement des risques cyber. L'idéal serait d'avoir un salarié qui serait en mesure de sensibiliser ses collègues dès leur entrée dans l'entreprise.

Ainsi, **ce manque de sensibilisation se traduit par de mauvaises pratiques informatiques qui réduisent drastiquement le niveau de sécurité global du SI.** Un salarié conscient des risques et vigilant constitue le premier rempart aux cybermenaces et saura donner l'alerte en cas d'anomalie. L'ANSSI souligne que la sensibilisation des collaborateurs permet de faire d'eux le premier pare-feu de de l'entreprise.

- **La stratégie de sauvegarde**

Une stratégie de sauvegarde inadéquate expose à des risques d'intégrité, de disponibilité et de confidentialité des données

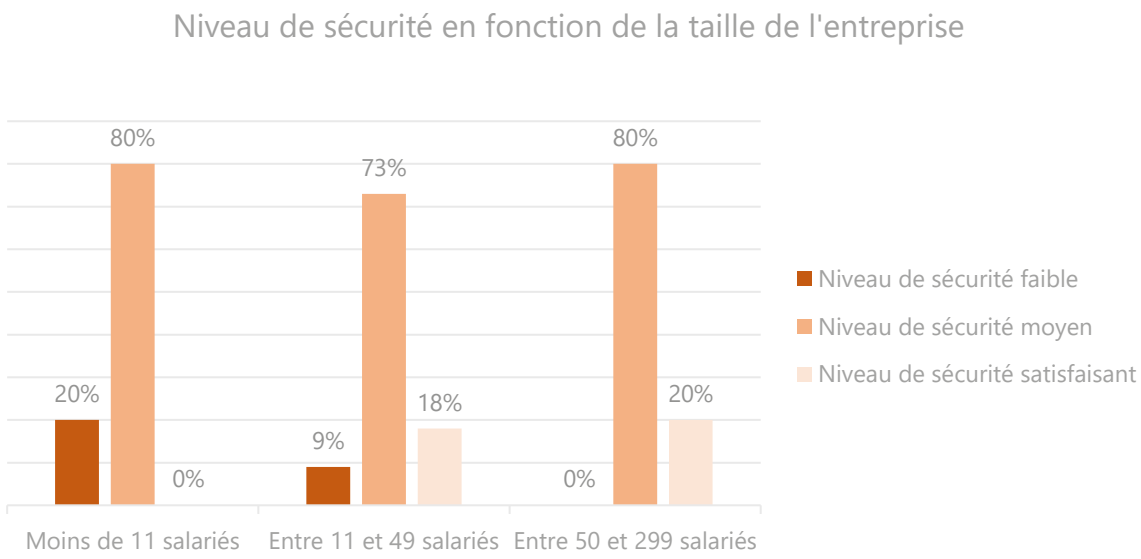
La sauvegarde des données de l'entreprise est un élément central. Pourtant, de nombreuses TPE/PME ont mis en œuvre une stratégie de sauvegarde qui n'est pas cohérente avec leurs objectifs.

Par exemple, une sauvegarde est réalisée une fois par semaine (elle conserve donc 7 jours) mais l'entreprise considère qu'elle peut perdre au maximum 2 jours de travail en cas de perte de données. De plus, **à plusieurs reprises, il a été constaté que des dirigeants transportaient des disques durs externes de sauvegardes non chiffrées dans leur sacoche.** Ces sauvegardes intègrent des données sensibles pour l'entreprise (données stratégiques, données personnelles, etc.).

En cas de vol, perte ou fuite de ces données, les impacts peuvent être conséquents (perte d'avantage concurrentiel, impact sur l'image de marque, sanction de la CNIL, perte financière, etc.).

4.2.3 Analyse par taille d'entreprise

En corrélant le niveau de sécurité des entreprises en fonction du nombre de salariés, les statistiques sont les suivantes :



Les statistiques révèlent que, **quel que soit le nombre de collaborateurs, la part d'entreprises ayant un niveau de sécurité "moyen" est identique**, cependant plus le nombre de collaborateurs augmente plus des niveaux de sécurités supérieurs semblent émerger.

Ce premier constat semble mettre en exergue le fait que **les mesures techniques/organisationnelles ainsi que le management de la sécurité du SI sont en partie corrélés à la taille de l'entreprise**.

La proportion d'entreprises ayant un niveau de sécurité "faible" est la plus importante dans les entreprises de moins de 11 collaborateurs (20%) contre 9% pour celles qui comptent entre 11 et 49 collaborateurs et 0% pour les entreprises au-delà de 50 salariés.

Le pourcentage d'entreprises ayant un niveau de sécurité satisfaisant est presque identique entre les entreprises de 11 à 49 collaborateurs et celles de 50 salariés et plus (18% et 20% respectivement). **Aucune des entreprises de moins de 11 salariés auditées ne possède un niveau de sécurité satisfaisant.**

En conclusion, entre les entreprises de moins de 11 salariés, celles entre 11 à 49 salariés et les entreprises de 50 salariés et plus, l'écart **est fonction des budgets consacrés à la mise en œuvre des mesures de sécurité** qui répondent aux besoins de l'entreprise. Naturellement, cela passe dans un premier temps par une prise de conscience des enjeux de cybersécurité et d'un engagement de la direction en matière de SSI.

Comme précisé dans l'article 3.1.2 un minimum de 7 entreprises était requis pour pouvoir distinguer les tendances propres à un secteur d'activité. Au vu du nombre d'entreprises impliquées par branche, hors-mis pour le Commerce à distance, il est peu pertinent et possiblement dangereux de faire des focus spécifiques par secteur d'activité.

4.3 Vers un Cyberdiag V2

L'expérimentation a donc eu pour objet de concevoir et de tester une démarche, une méthode et un ensemble d'outils dans le but de proposer une prestation Cyberdiag adaptée aux entreprises du commerce et de la distribution.

4.3.1 Constats et recommandations

En cette fin d'expérimentation du Cyberdiag, le retour d'expérience des entreprises a été analysé afin d'en tirer des constats et ainsi proposer des ajustements et améliorations.

- **Communication :**

Pour déployer plus largement le Cyberdiag et intéresser les TPE/PME à la cybersécurité, la communication est un enjeu majeur. En complément de la vidéo de présentation du Cyberdiag, il pourrait être pertinent de communiquer plus largement auprès des adhérents de l'Opcommerce :

  - Apparaitre dans une newsletter de l'Opcommerce,
  - Relayer l'action sur les réseaux sociaux professionnels,
  - Publier des bannières web sur les sites des partenaires et parties prenantes.

- **Autodiag :**

Afin de permettre une notation pertinente et un rendez-vous sur site pertinent et efficace, l'Autodiag est exhaustif et important pour le déroulé du diagnostic dispensé par le consultant. Cette étape doit être rendue obligatoire.

- **Tutos :**

Les tutos ont été appréciés par les entreprises qui les ont téléchargés. La visibilité de ces documents sur l'espace personnel pourrait être améliorée afin qu'aucune entreprise de ne passe à côté.

- **Référentiel :**

Le référentiel (outil compilant les thématiques, les points d'observation et les niveaux associés en matière de cybersécurité permettant la conduite d'entretiens par les consultants)

créé en début de projet est bien adapté aux TPE/PME du commerce et de la distribution. Les consultants suggèrent néanmoins d'approfondir les questions liées au RGPD qui reste un sujet d'actualité car toutes les entreprises ne sont pas encore en conformité.

- **Rapport Cyberdiag :**

Le rapport de fin de diagnostic a reçu un accueil très positif aussi bien sur le fond que sur la forme. Néanmoins une amélioration graphique de la présentation des résultats détaillés pourrait faciliter la lecture et l'assimilation de l'information.

- **Livraison du rapport :**

Pour des raisons évidentes de sécurité, les rapports sont livrés par email dans un conteneur chiffré. Cela implique que le destinataire du rapport télécharge et installe un petit logiciel. La marche à suivre est détaillée dans l'email accompagnant le document.
Phosforea recommande de mettre en place une plateforme de téléchargement sécurisée pouvant faciliter cette étape pour l'entreprise et évitant ainsi l'installation d'un programme sur le poste de travail.

- **Restitution téléphonique :**

La bonne qualité du rapport produit a eu pour effet un faible nombre de questions de la part des entreprises lors de la phase de restitution téléphonique. Cette étape était néanmoins nécessaire pour expliquer la démarche d'accompagnement à venir et aider l'entreprise à se positionner sur la suite de la prestation.

- **Découpage du temps de la prestation :**

La répartition temporelle des différentes étapes de la prestation telle que prévue initialement (cf 2.1.3) a connu une réalité différente sur le terrain. En effet, la phase d'entretien sur site a duré en moyenne près de 3 heures selon la taille de l'entreprise et non pas de 0,5 à 1 jour. A l'inverse, le temps de rédaction du rapport a été sous-estimé et selon la maturité de l'entreprise le temps imparti à cette tâche était en moyenne de 1,5 jour.

- **Accompagnement :**

Toutes les entreprises n'ont pas souhaité bénéficier de l'accompagnement renforcé. Le constat principal fait sur la phase d'accompagnement est le temps moyen de l'exécution des prestations par entreprise : 72 jours d'accompagnement pour 18 entreprises soit une moyenne de 4 jours d'accompagnement par entreprise.

- **Suivi à 1 mois :**

Cet appel téléphonique ayant lieu un mois après la restitution du rapport a eu un intérêt limité pour 2 raisons :

- Les entreprises choisissant un accompagnement bénéficiaient d'un suivi rapproché de la part du prestataire qui étaient donc informé de l'avancement de la mise en œuvre du plan d'action et des intentions futures.
- En cybersécurité, il y a parfois des actions à mener rapidement mais la mise en œuvre d'un plan d'action peut s'étaler sur plusieurs mois car il peut nécessiter des moyens humains et financiers.

- **Disponibilité des entreprises :**

Un point a été sous-estimé : le nombre de relances, appels, emails nécessaires pour joindre une entreprise ou convenir des divers rendez-vous ponctuant le Cyberdiag. Les dirigeants sont souvent peu disponibles (report de rendez-vous, taux de réponse faible…) ce qui a engendré un temps de gestion de projet supérieur à ce qui avait été prévu au début de l'expérimentation. Ceci est un facteur à prendre en compte pour la suite.

4.3.2 Un Cyberdiag adapté

Des recommandations pour un Cyberdiag amélioré et adapté aux spécificités des TPE/PME du commerce et de la distribution : Phosforea propose une prestation fixe de 5 jours (temps consultant) par entreprise (de moins de 300 salariés) demandant la prestation avec la distribution temporelle suivante :

- 0,5 jour : diagnostic sur site
- 1,5 jour : rédaction du rapport
- 3 jours : accompagnement approfondi (optionnel)

Proposition Cyberdiag V2– Parcours TPE/PME

1. Rendez-vous téléphonique initial
2. Signature d'une convention d'audit tripartite, autorisation préalable à toute intervention dans l'entreprise
3. Réponse à l'Autodiag et consultation des tutos : incontournables
4. Visite sur site (audit/diagnostic) + signature feuille d'émargement
5. Rapport Cyberdiag
6. Restitution téléphonique
7. Accompagnement (optionnel)
8. Signature de la feuille d'émargement

5. Conclusion

L'expérimentation du Cyberdiag menée sur 26 entreprises du territoire national, TPE/PME du secteur du commerce et de la distribution, a permis de structurer une démarche pragmatique d'accompagnement à la prise en compte des risques et de la cybersécurité pour cette typologie d'entreprises.

Deux enseignements principaux doivent en être retenus :

- Tout d'abord, le **haut niveau d'exposition aux risques de cybermenaces des TPE/PME** françaises : 100% des entreprises ayant pris part à l'expérimentation ont été victimes de cyber-attaques (tentative ou attaques abouties) dans les mois précédent l'accompagnement ;
- Par ailleurs, **le très faible niveau de prise de conscience des dirigeants face aux risques** : certains incidents de sécurité ne sont pas reportés comme des cyberattaques car non reconnus comme tels. Leur impact sur le fonctionnement de l'entreprise est largement sous-estimé et le suivi en termes de remédiation ou de non-réplication est quasi-nul.

Si dans toutes les entreprises il est vrai de dire que l'utilisateur du système d'information, c'est-à-dire le salarié, est un maillon essentiel contre les attaques informatiques, dans le cas des TPE/PME, la personne-clé est clairement le dirigeant. C'est en effet 'le patron' qui doit être la cible de toutes les actions d'accompagnement et de sensibilisation pour une plus grande prise en compte des risques de cybersécurité.

La sensibilisation du dirigeant est apparue comme un point clé de cette expérimentation, mais ce n'est pas le seul intérêt du projet, elle a, par son côté pragmatique et son approche terrain, permis aux TPE/PME participantes de comprendre les risques principaux qui pèsent sur leur business, et de formaliser, en un temps record et avec un investissement minimal de leur part, les bases d'une politique interne de sécurité.

C'est un des grands succès de ce dispositif : donner les clés pour parer au plus urgent et mettre à l'abri, dans une logique 'quick-win' (Plan d'action qui vise à améliorer les défauts d'organisation d'une entreprise), le patrimoine de ces TPE/PME.