apave

Renforcer la cybersécurité des TPE PME françaises :
Restitution de notre enquête 2023
et guide pratique !

Depuis ces 2 dernières années, les cyberattaques ont été largement médiatisées. Les solutions de protection contre les cybermenaces se sont multipliées. Les TPE & PME, entre autres, ont été particulièrement ciblées.

SOMMAIRE

INTRODUCTION

Le groupe Apave, en partenariat avec ITrust, Free Pro, et sous l'égide de la Fédération Française de la Cybersécurité, a mené une enquête nationale auprès des TPE et PME françaises afin d'évaluer leur niveau de maturité actuel en matière de cybersécurité et de comparer son évolution au cours des deux dernières années, compte tenu des cyberattaques importantes et médiatisées ayant eu des conséquences dramatiques.

Notre objectif est de vous sensibiliser et de vous accompagner en vous fournissant un plan de communication et d'accompagnement adapté à votre niveau de maturité. Ce plan vise à vous aider à prendre conscience des risques liés aux cyberattaques et à mettre en place des dispositifs de protection efficaces.

En première partie de ce document, vous trouverez les résultats détaillés de cette enquête, vous permettant ainsi d'évaluer le niveau de sécurité de votre entreprise et de prendre les mesures nécessaires pour renforcer efficacement votre protection contre les cyberattaques. De plus, nous avons comparé ces résultats avec ceux de notre enquête réalisée en 2021, ce qui met en évidence votre prise de conscience croissante des problématiques liées à la cybersécurité au sein des petites et moyennes entreprises.

En seconde partie de ce document, vous retrouverez notre approche unique pour mieux maîtriser les risques numériques, y compris les risques de cyberattaques. À partir de cette approche et des éléments recueillis lors de nos enquêtes, nous avons élaboré une fiche pratique spécialement conçue pour les TPE et PME. Cette fiche pratique vous accompagnera dans votre démarche en vous fournissant des conseils étape par étape, des bonnes pratiques et des ressources utiles pour renforcer la sécurité informatique de votre entreprise.

Nous sommes convaincus que ce guide vous aidera à approfondir votre compréhension des enjeux de la cybersécurité et à mettre en place des mesures concrètes pour faire face aux risques numériques, notamment les cyberattaques.

Je vous souhaite une agréable lecture,
Harold Huillier, Directeur Délégué du groupe Apave Digital

apave

Partie 1/

Restitution de l'enquête

1 Contexte

Dans cette section, nous allons vous présenter les objectifs de cette enquête, la méthodologie utilisée ainsi que les profils des participants qui ont contribué à cette étude.

1 Contexte

Cette enquête a été menée par le groupe **Apave**, en partenariat avec **ITrust** et **Free Pro**, et sous l'égide de la **Fédération Française de la Cybersécurité**.

4 semaines d'ouverture — Avril 2023 → Mai 2023

Objectifs de cette enquête :

1. **Évaluer le niveau de maturité des TPE & PME** en matière de cybersécurité.

2. **Comparer l'évolution du niveau de maturité des TPE & PME** en matière de cybersécurité au cours des deux dernières années, suite à notre précédente enquête réalisée en 2021.

1 Structure de l'enquête

Nous avons conçu une enquête spécifique destinée aux TPE et PME, comprenant 50 questions réparties en 3 sections.

50
Questions

1 Les entreprises ayant déjà été victimes d'une cyberattaque

Dans cette section, nous avons interrogé les entreprises pour déterminer si elles ont déjà été victimes ou non d'une cyberattaque. En fonction de leurs réponses, nous leur avons posé des questions complmentaires sur le contexte et les conséquences de l'attaque subie, ou à défaut, sur leurs craintes face à une éventuelle cyberattaque.

2 Leur organisations en cybersécurité

Dans cette section, nous examinons l'organisation des entreprises en matière de cybersécurité, en nous intéressant à plusieurs aspects clés : la présence d'équipes dédiées, le budget alloué, la couverture d'assurance, ainsi que la mise en place d'une stratégie RGPD visant à protéger les données en cas de cyberattaque et à se conformer à la réglementation.

3 Leur plan d'action en cybersécurité

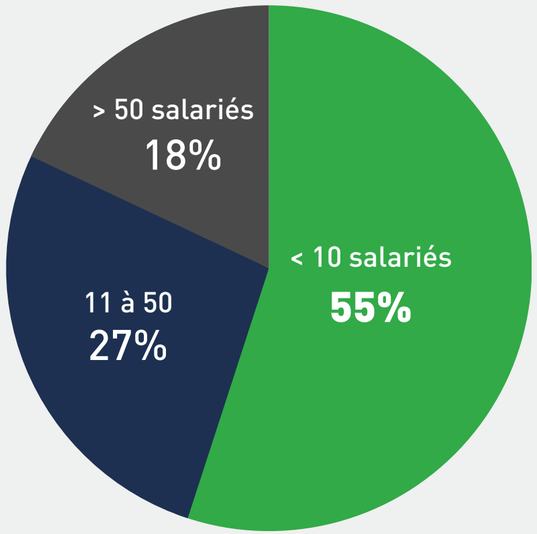
Dans cette dernière partie de l'enquête, nous examinons les mesures de protection mises en place par ces entreprises afin de faire face aux risques cyber, telles que la réalisation de diagnostics de cybersécurité, la formation de leurs équipes aux bonnes pratiques, ainsi que la réalisation de campagnes de phishing pour évaluer leurs employés dans des situations réelles.

1 Profils des répondants

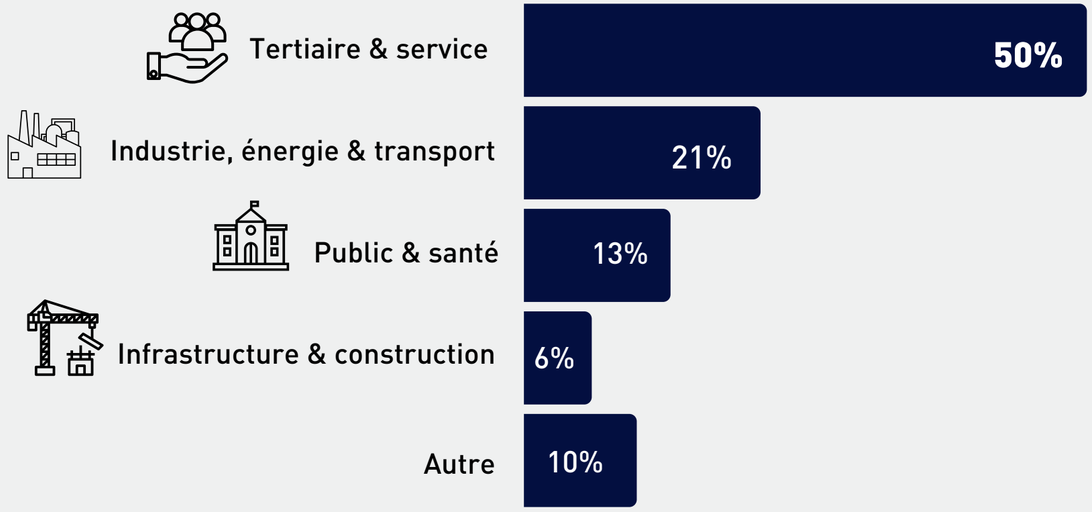
541
Réponses analysées

Cette enquête a été diffusée aux clients des sociétés Apave, ITrust & Free Pro.
Une vérification a été effectuée pour exclure de l'analyse les organisations dont l'effectif dépasse 250 collaborateurs, afin de maintenir la dimension TPE et PME.

Répartition par effectif :



Répartition par secteur d'activité :



2

Les TPE PME victimes d'une cyberattaque

Dans cette section, nous avons interrogé les entreprises pour déterminer si elles ont déjà été victimes ou non d'une cyberattaque. En fonction de leurs réponses, nous leur avons posé des questions complémentaires sur le contexte et les conséquences de l'attaque subie, ou à défaut, sur leurs craintes face à une éventuelle cyberattaque.

2 Les TPE PME victimes de cyberattaques

Analyse des cyberattaques rencontrées

21%

Des entreprises interrogées ont déjà été victimes d'une cyberattaque !

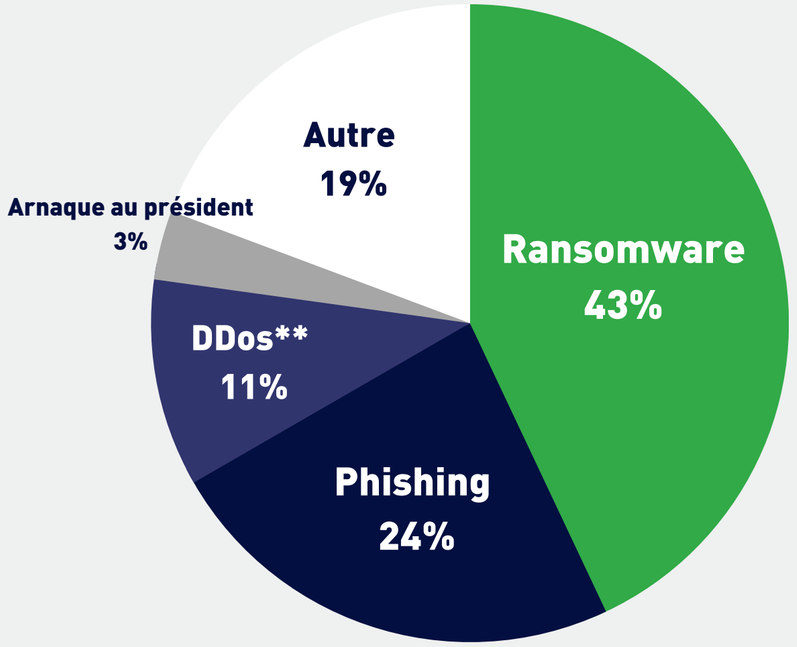
Soit 114 entreprises de notre panel.
(Elles étaient 23% en 2021*)

- **14%** pour les TPE < 10 salariés
- **39%** pour les PME > 50 salariés

Les plus grandes entreprises restent les principales cibles, mais les TPE ne sont pas pour autant épargnées.

*enquête Apave réalisée en 2021

Répartition par typologie de cyberattaque :



**L' attaque par Déni de Service Distribué bloque l'accès à un service tel qu'un serveur ou un site web

On retrouve notamment dans la catégorie "autre", les verbatims suivants :

- Le piratage du site web
- Le piratage du téléphone
- Par le biais d'un fournisseur "infecté"

70%

Des cyberattaques passent par le biais du salarié !

(46% en 2021* selon notre enquête)

Les collaborateurs des entreprises sont donc des cibles privilégiées par des hackers, **<u>à sensibiliser et à former</u> régulièrement pour maintenir votre sécurité** !

2 Les TPE PME victimes de cyberattaques

Les mesures prises

Des entreprises ont mis en place de nouvelles mesures à la suite de cette attaque.

Parmi les principales actions mises en œuvre, on retrouve :

- **Des actions de sensibilisation auprès des collaborateurs,** notamment par le biais de la formation (dans 55% des cas).
- **Des améliorations sur la sécurité des systèmes**, avec la mise en place de pare-feu, antivirus ou encore des systèmes de sauvegarde automatisés (dans 45% des cas).

Des entreprises victimes d'une cyberattaque n'ont pas mis en place de nouvelles mesures pour mieux se protéger !

Le constat est préoccupant : le fait d'avoir déjà été victime d'une attaque ne garantit en rien qu'une entreprise ne soit pas à nouveau ciblée. Une fois que la pression de l'attaque subie retombe, **les entreprises ont tendance à se remettre rapidement à leurs activités quotidiennes sans entreprendre les améliorations nécessaires** suite à cette expérience malheureuse.

apave

2 Les TPE PME victimes de cyberattaques

Les principales conséquences

1 Indisponibilité des systèmes et services

- Arrêt de la production
- Indisponibilité du site web
- Blocage du système d'information

57% Ce blocage est < à 1 journée

43% Ce blocage est > à 1 journée
Dont 10% + de 10 jours

2 La perte financière directe

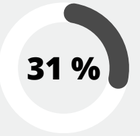
- Prélèvements frauduleux
- Introduction dans le système bancaire

3 Le vol de données

Toutes les données intéressent aujourd'hui les hackers !
Répartition des types de données volées :

Données de produits ou services

Données clients



Données collaborateurs

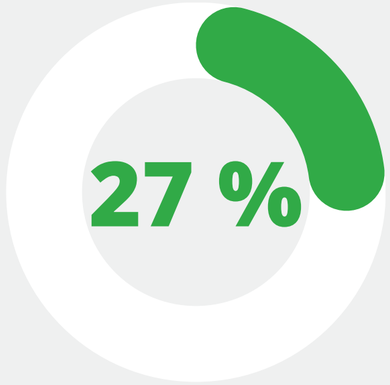
100%

Pour 100% des cas, nous observons une perte financière à la suite de cette attaque, qu'elle soit de manière directe ou indirecte !

Parmi les autres conséquences identifiées, nous retrouvons notamment **des effets négatifs sur la réputation et l'image de l'entreprise.**

2 Les TPE PME victimes de cyberattaques

À la suite de cette attaque



Des entreprises ont porté plainte à la suite de cette attaque

Des entreprises ayant porté plainte ont été indemnisées par leur assurance

Pour rappel, depuis le **24 avril 2023**, toute personne physique ou morale victime de pertes ou de dommages causés par une cyberattaque dans le cadre de son activité professionnelle devra **porter plainte dans un délai de 72 heures à compter de la connaissance de cette atteinte pour pouvoir être indemnisée par son assureur.**
(Source : https://entreprendre.service-public.fr/)

Par ailleurs, **en cas de violation de données à caractère personnel, conformément à l'article 33 du RGPD,** il convient de **notifier l'incident à la CNIL dans un délai de 72 heures** via le site dédié de la CNIL.

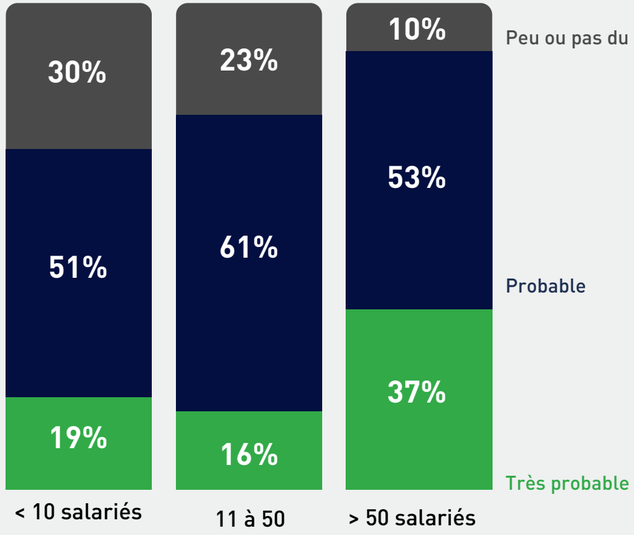
2 Pour les entreprises n'ayant jamais été victimes

Des entreprises pensent ne pas être une cible potentielle pour les hackers !

Elles représentaient 70% en 2021, ce qui témoigne d'une prise de conscience en progression des enjeux cyber au sein des TPE et PME.

Cela souligne également la nécessité de poursuivre les efforts pour sensibiliser l'ensemble des entreprises et renforcer leur préparation face aux cyberattaques.

Avec une disparité selon l'effectif de l'entreprise :



Près de 10% des entreprises de plus de 50 salariés ne se sentent pas concernées par le risque de cyberattaque, ce qui met en évidence la nécessité de sensibiliser davantage, y compris les entreprises de taille plus importante.

Les plus grandes craintes de ces entreprises face à une potentielle cyberattaque :

- **53 %** Vol, perte ou fuite de données
- **19 %** Fermeture de l'entreprise
- **11 %** Perte financière directe
- **7 %** Dévalorisation de l'image de l'entreprise
- **10 %** Autre (paralysie du SI, ransomware...)

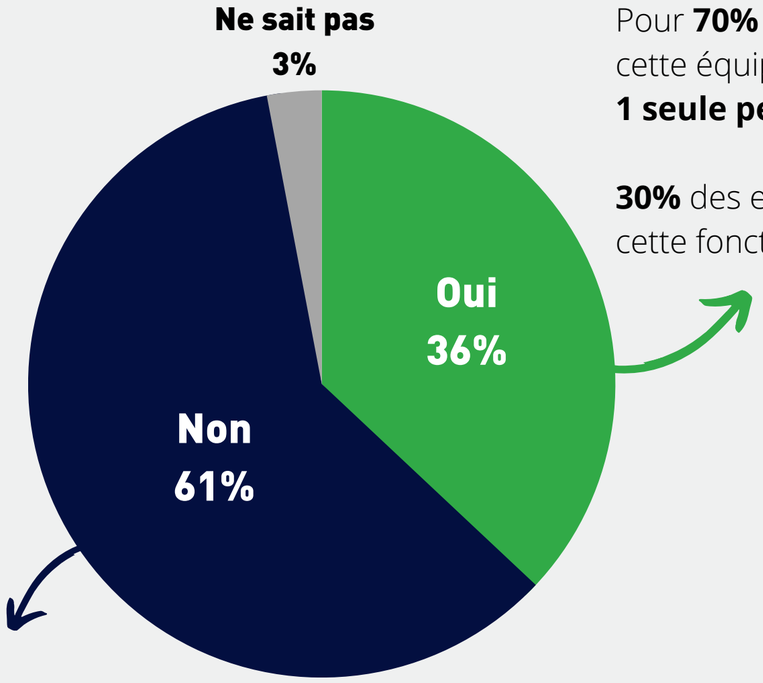
Certaines entreprises ont une bonne compréhension des enjeux cyber. Il est maintenant essentiel qu'elles passent à l'action en mettant en place des mesures concrètes pour renforcer leur sécurité.

3 Organisation

Dans cette section, nous examinerons l'organisation des entreprises en matière de cybersécurité, en nous intéressant à plusieurs aspects clés : la présence d'équipes dédiées, le budget alloué, la couverture d'assurance, ainsi que la mise en place d'une stratégie RGPD visant à protéger les données en cas de cyberattaque et à se conformer à la réglementation.

3 L'organisation en cybersécurité

Entreprises ayant une équipe dédiée à la cybersécurité :



Pour **70%** d'entre elles, cette équipe est composée de **1 seule personne**

30% des entreprises externalisent cette fonction.

Cette part monte à **70%** pour les entreprises **< 10 salariés**

Budget et assurance :

93%

des TPE et PME n'ont pas de budget spécifiquement alloué à la cybersécurité, distinct du budget informatique.

De manière générale, le budget cybersécurité est directement intégré au budget informatique de l'entreprise.

25%

des TPE PME déclarent avoir une couverture assurance en cas de cyberattaque.

Par ailleurs**, 40%** des entreprises ne savent pas si elles sont couvertes par leur assurance en cas de cyberattaque.

3 Les documents mis en place

De prévention et gestion du risque cyber

47%

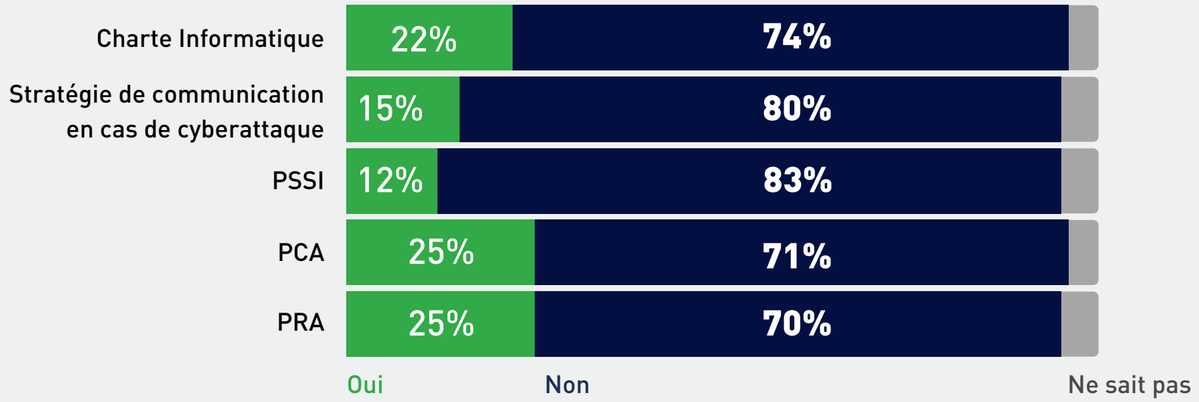
des TPE PME n'ont aucun document cyber mis en place au sein de leur structure.

11%

des entreprises ont mis en place l'ensemble de ces documents :

- **Charte informatique**
- **Stratégie de communication** en cas de cyberattaque
- **PSSI** : Politique de Sécurité des Systèmes d'Information
- **PCA** : Plan de Continuité d'Activité
- **PRA** : Plan de Reprise d'Activité

Zoom sur les documents mis en place dans les entreprises < 10 salariés :



3 Les documents mis en place

De prévention et gestion du risque cyber

40%

des TPE PME ont mis en place une charte informatique

- **22%** pour les TPE < 10 salariés
- **75%** pour les PME > 50 salariés

Plus l'effectif est important, plus les formalités de gestion du risque cyber sont mises en œuvre.
Dans **95%** des cas, cette charte est diffusée en interne.

21%

ont mis en place une stratégie de communication en cas de cyberattaque

« Lorsqu'une crise cyber survient, l'action des communicants passe trop souvent au second plan. C'est une erreur. Pour une gestion globale de la crise, il est indispensable que la communication travaille main dans la main avec la réponse technique. »
Guillaume Poupard, ancien directeur général de l'ANSSI

20%

ont mis en place une PSSI (Politique de Sécurité des Systèmes d'Information)

Une PSSI est document de référence reflétant la vision stratégique et les objectifs d'une organisation en matière de sécurité des systèmes d'information (SSI) et détermine les règles de sécurité à adopter. C'est une démarche opérationnelle et stratégique.

30%

ont mis en place un PCA (Plan de Continuité d'Activité)

Le PCA a pour objectif de maintenir la disponibilité du système d'information (SI) en cas d'attaque et ainsi assurer la continuité des activités pour l'entreprise.

32%

ont mis en place un PRA (Plan de Reprise d'Activité)

Le PRA détaille les différentes procédures et les moyens techniques à mettre en œuvre en cas d'attaque, avec pour objectif de reprendre rapidement l'activité.

3 Politique de sécurité

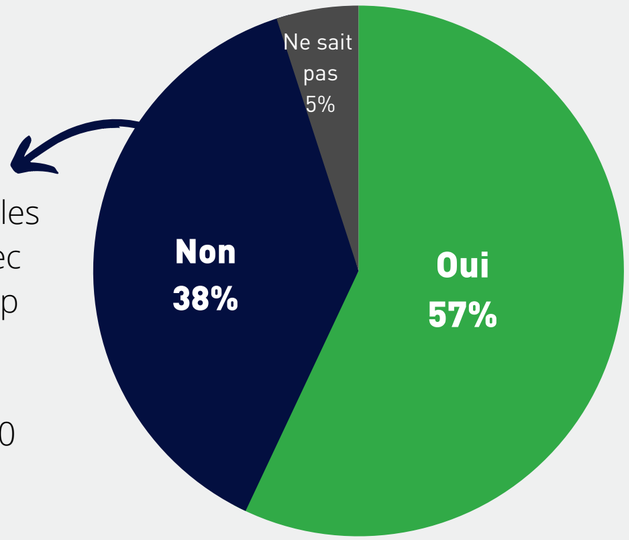
Pour les appareils mobiles et les accès distants

Sont comptabilisés parmi les appareils mobiles :

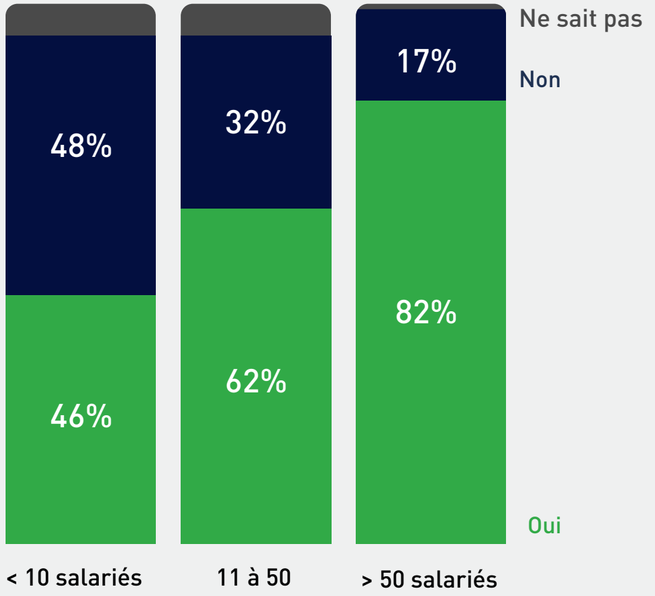
- Les ordinateurs portables
- Les téléphones portables
- Les tablettes, ...

Ces **politiques de sécurité** - pourtant indispensables pour garantir la sécurité numérique notamment avec la **multiplication du télétravail -** sont encore trop peu mises en oeuvre par les entreprises, exposant ainsi leurs données à des risques importants.
Sont principalement concernées les entreprises < 50 salariés.

Entreprises ayant mis en place une politique de sécurité pour les appareils mobiles et les accès distants :



Avec une disparité selon l'effectif de l'entreprise :



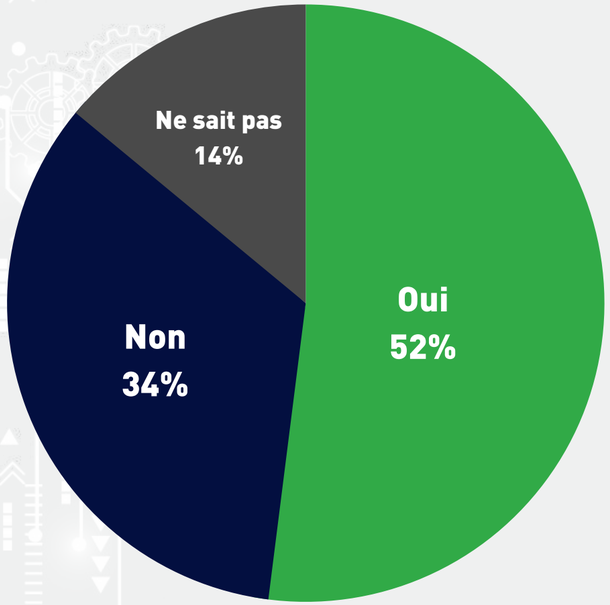
En mettant en place des mesures de sécurité indispensables pour les appareils mobiles, telles que **l'authentification à deux facteurs (MFA), le chiffrement des données via un VPN** (Virtual Private Network) et **l'utilisation de réseaux Wi-Fi sécurisés,** les entreprises peuvent **renforcer leur sécurité et protéger leurs informations confidentielles.**

3 Le RGPD

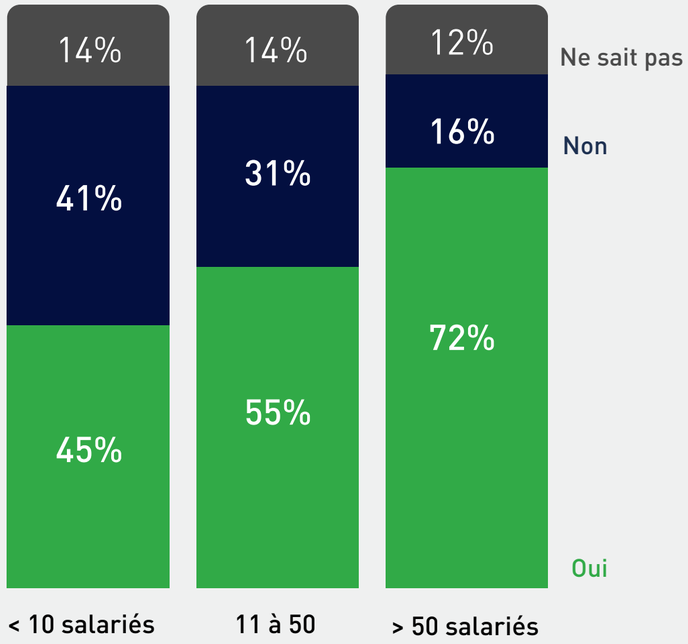
Règlement Général sur la Protection des Données

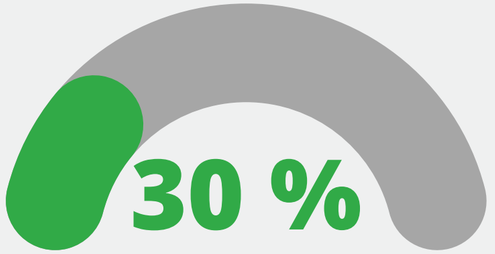
Le RGPD, entré en vigueur le **25 mai 2018**, vise à renforcer la protection des données personnelles des citoyens de l'Union Européenne et à harmoniser les lois sur la protection des données. Pour rappel, **le RGPD est obligatoire et applicable pour l'ensemble des entreprises et organisations traitant des données de ressortissant européens**.

Entreprises ayant mis en place une stratégie RGPD :



Avec une disparité selon l'effectif de l'entreprise :





Des entreprises ont désigné un Délégué à la Protection des Données (DPO)

La désignation d'un DPO est obligatoire dans certains cas, notamment :

- Pour les organismes publics
- Pour les organismes dont les activités donnent lieu à un traitement de masse, systémique et régulier des données
- Pour les organismes traitants des données personnelles sensibles

Indirectement lié à la cybersécurité, le RGPD favorise la réduction des risques et l'atténuation des conséquences des pertes de données lors de cyberattaques, grâce à des mesures de sécurité plus strictes mises en place par les entreprises.

Découvrir notre accompagnement

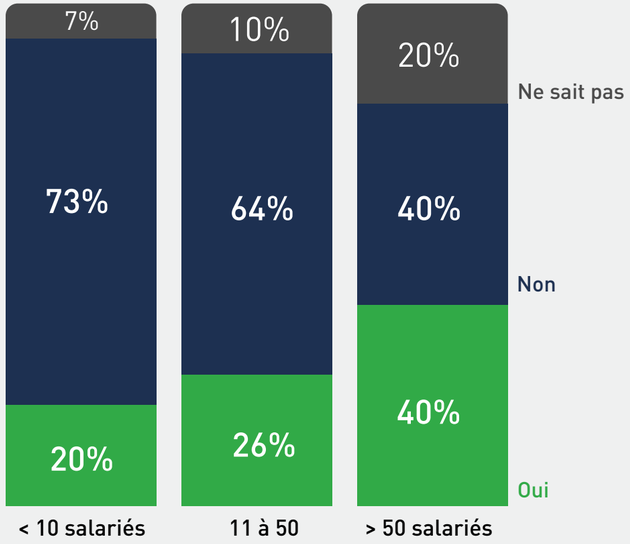
4 Plan d'action

Dans cette dernière partie de l'enquête, nous examinerons les mesures de protection mises en place par ces entreprises afin de faire face aux risques cyber, telles que la réalisation de diagnostics de cybersécurité, la formation de leurs équipes aux bonnes pratiques, ainsi que la réalisation de campagnes de phishing pour évaluer leurs employés dans des situations réelles.

4 Le plan d'action cyber

des entreprises n'ont pas mis en place de plan d'action cyber au sein de leur structure !

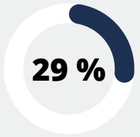
Avec une disparité selon l'effectif de l'entreprise :



Principales raisons pour lesquelles le plan d'action n'a pas été élaboré :

Elles ne savent pas comment démarrer leur plan d'action

Elles étaient 37% à ne pas savoir comment démarrer en 2021.



Ce n'est pas un sujet prioritaire pour elles

Elles étaient 28% en 2021.

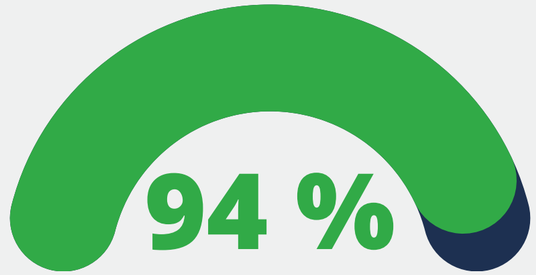
Elles n'ont pas de budget dédié à consacrer

Autre :
Ressources insuffisantes, manque de temps à accorder, peu de risques perçus...

Les faibles progrès récents dans les entreprises en matière de cybersécurité soulèvent des interrogations sur la sensibilisation et les défis persistants à surmonter.

4 Les antivirus / antimalwares

Pour 90% des entreprises, les postes de travail sont équipés de protection contre les logiciels malveillants (antivirus, antimalware)



Dans 94% des cas, le répondant pense que ces logiciels sont bien mis à jour.

ATTENTION

> Un **antivirus** ou **antimalware** qui n'est **pas à jour** est **inutile voire dangereux** pour vos ordinateurs !

> Pour fonctionner, un antivirus s'appuie sur une **base de données virales**, c'est à dire **la liste des menaces connues et répertoriées**.

> Il est donc primordial de s'assurer de leurs **mises à jour automatiques et régulières** !

4 La sauvegarde des données

94%

des entreprises effectuent des sauvegardes de leurs données

66%

des entreprises vérifient la qualité de leur sauvegarde :

- **62%** Pour les entreprises < 10 salariés
- **80%** Pour les entreprises > 50 salariés

La sauvegarde des données constitue une mesure fondamentale pour se prémunir contre les cyberattaques. Elle permet la restauration des données, la prévention des pertes et la continuité des activités en cas d'incident. Ainsi, il est recommandé d'utiliser du matériel approprié, tel que **des solutions intégrant la sauvegarde, la restauration, la protection contre les malwares et la gestion de la sécurité des postes de travail.**

Moyen de sauvegarde utilisé :

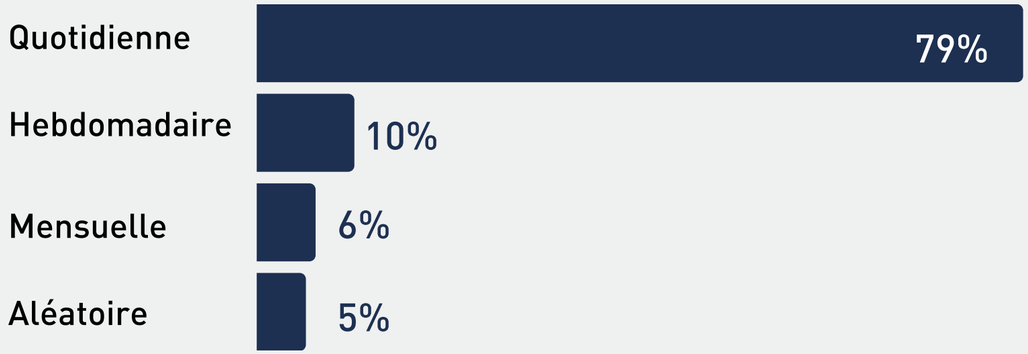
40 % Par le cloud

38 % Par le réseau (via un NAS par exemple)

Un serveur NAS (Network Attached Storage) est un appareil de stockage et de partage de fichiers relié à un réseau local ou à internet.

22 % Par du matériel (clé USB, disque dur, etc.)

Fréquence des sauvegardes :



4 Les accès wifi pour les visiteurs

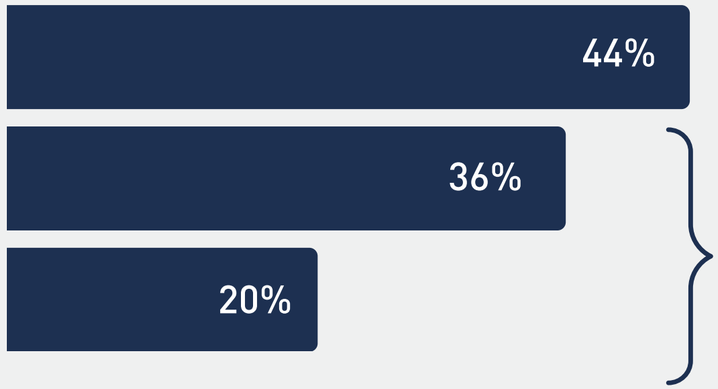
La connectivité sans fil est devenue un élément important dans les usages et la mise à disposition d'accès wifi par les entreprises pour leurs visiteurs est devenue pratique courante.

59%

des entreprises mettent à disposition un accès wifi pour les visiteurs

- **42%** Pour les entreprises < 10 salariés
- **79%** Pour les entreprises > 50 salariés

Par quel moyen :



Ces pratiques peuvent entraîner des vulnérabilités et une éventuelle exploitation des infrastructures internes par des attaquants.

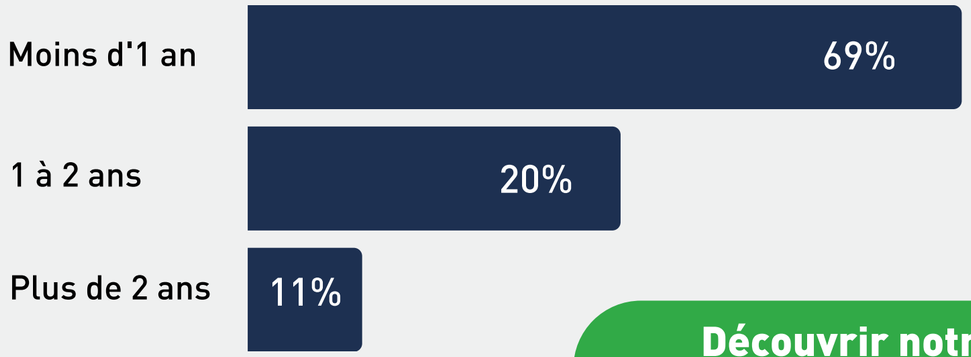
4 Action mise en œuvre par les TPE PME

Le diagnostic de cybersécurité

25% **des entreprises ont réalisé un diagnostic de cybersécurité**

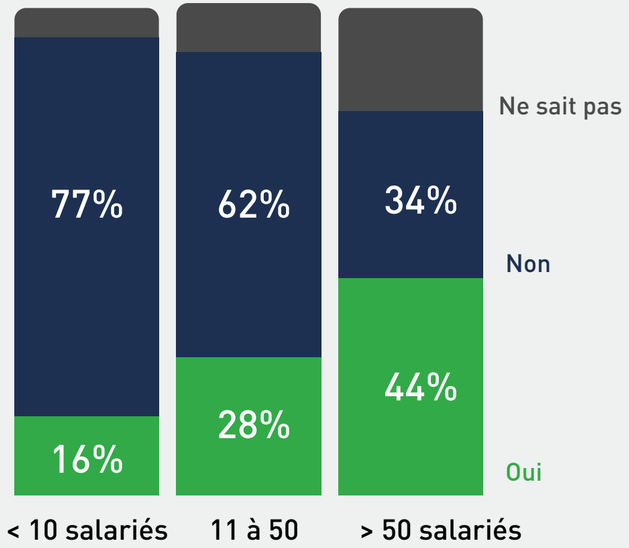
- **41%** avec des outils en ligne
- **59%** en faisant appel à un prestataire

Date du dernier diagnostic effectué :



Découvrir notre diagnostic CYBER

Avec une disparité selon l'effectif de l'entreprise :



Pourtant plébiscité, l**e diagnostic de cybersécurité est encore insuffisamment effectué par les entreprises, alors qu'il constitue la première étape essentielle** pour évaluer le niveau de sécurité informatique d'une structure et mettre en place des mesures correctives contre les risques identifiés.

4 Action mise en œuvre par les TPE PME

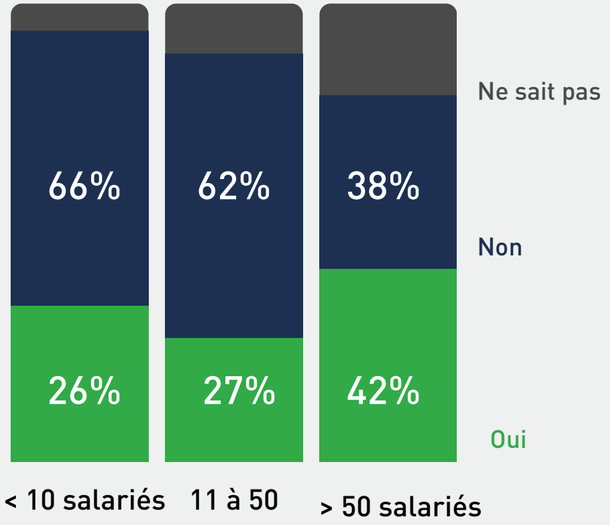
Le scan de vulnérabilité

29%

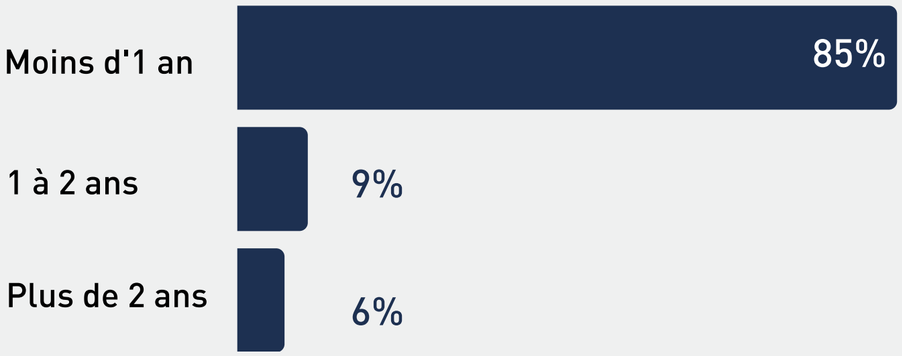
des entreprises ont réalisé un scan de vulnérabilité

Le site web est une ressource essentielle pour les TPE et PME. Il constitue une vitrine en ligne avec une visibilité accrue, une opportunité de communication avec les clients et une plateforme pour promouvoir les produits et services.
A l'inverse, il représente également une porte d'entrée pour les hackers.

Avec une disparité selon l'effectif :



Date du dernier scan effectué :



Aujourd'hui, la majorité des TPE PME n'ont pas effectué de scan de vulnérabilité, alors que **le site web d'une entreprise, qu'il soit marchand ou non, représente une ressource stratégique.** Il est l'une des principales cibles en cas de cyberattaque.

Découvrir notre scan de vulnérabilité

4 Action mise en œuvre par les TPE PME

Les formations en cybersécurité

44%

des entreprises ont formé leurs collaborateurs aux bonnes pratiques de cybersécurité.

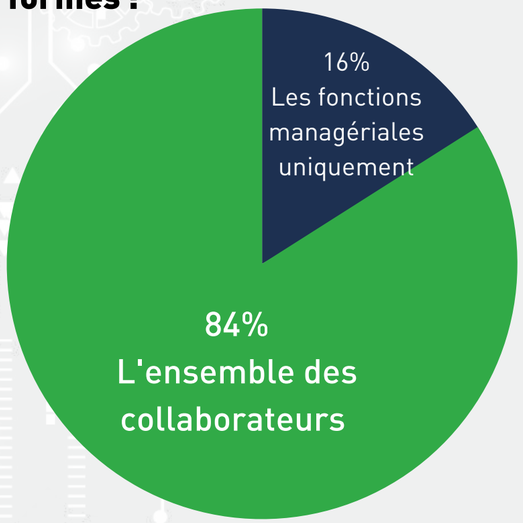
L'humain est la 1ère porte d'entrée d'une cyberattaque réussie ! Former vos collaborateurs devient donc indispensable et permet de :

- **Sensibiliser** aux enjeux cyber
- **Partager les bonnes pratiques** en interne
- **Amener à la prise de conscience** individuelle**.**

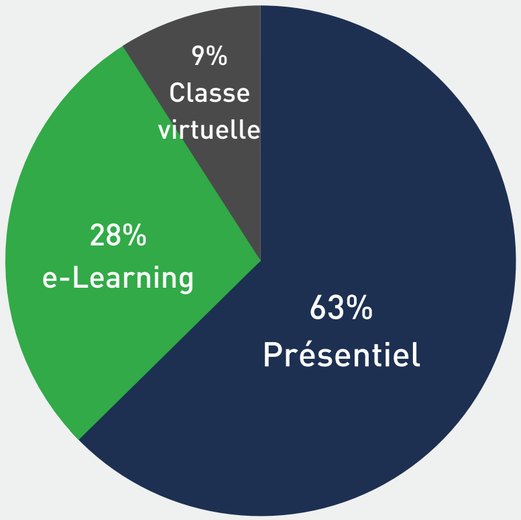
Découvrir nos formations dédiées aux salariés

Découvrir nos formations dédiées aux managers

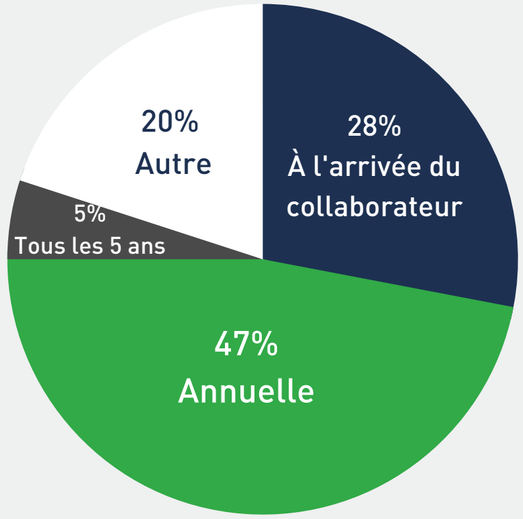
Répartition des collaborateurs formés :



Modalités de la formation :



Fréquence de la formation :



Les formations en cybersécurité proposées par le groupe Apave sont disponibles en différents formats :

- **Présentiel**
- **e-Learning**
- **Classe virtuelle**

4 Action mise en œuvre par les TPE PME

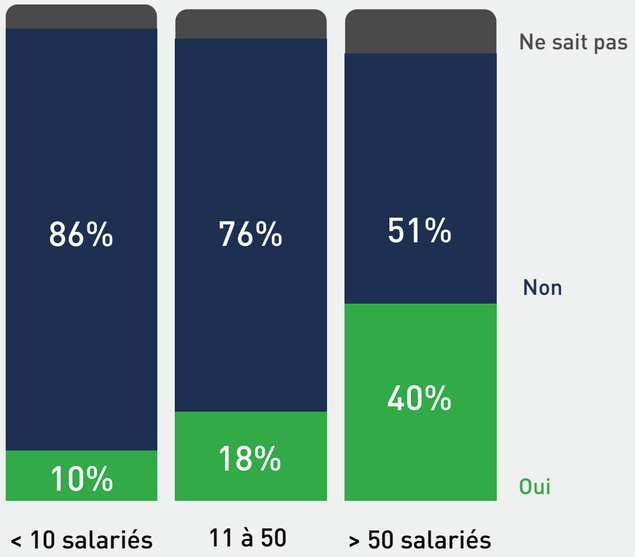
Les campagnes de phishing

17%

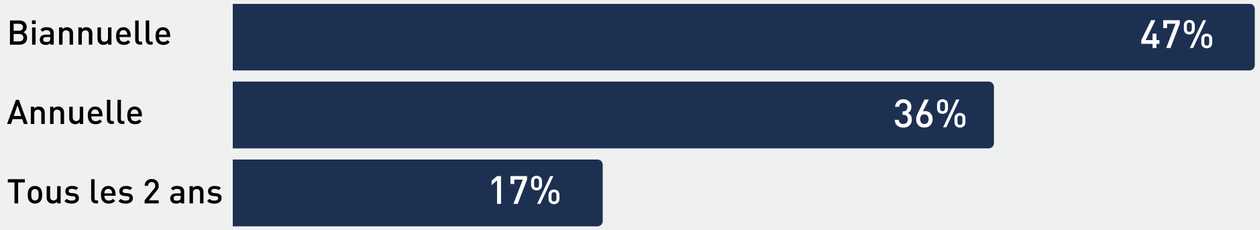
des entreprises ont mené des campagnes de phishing auprès de leurs salariés.

La campagne de phishing permet de tester les réactions de vos collaborateurs en situation de cyberattaque et de mener des actions de sensibilisation selon les résultats observés. **Leur réalisation régulière permet de maintenir à niveau les collaborateurs aux techniques d'attaque et de renforcer leur résilience contre ces menaces continues.** Les campagnes peuvent être personnalisées selon le secteur d'activité de l'entreprise et selon les profils des collaborateurs : c'est un véritable test grandeur nature !

Avec une disparité selon l'effectif :



Fréquence des campagnes menées :



Découvrir nos campagnes de phishing

4 L'accompagnement en cybersécurité

Répondre aux attentes des TPE PME

52%

des entreprises ne sentent pas assez accompagnées en cybersécurité !

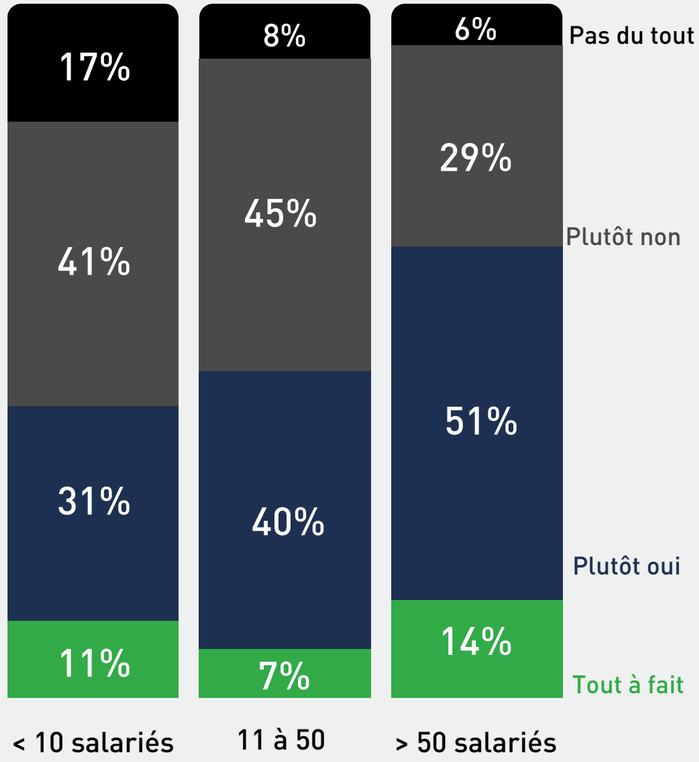
Malgré le développement de nombreuses solutions en cybersécurité sur le marché et les efforts d'accompagnement des pouvoirs publics, **plus de la moitié des TPE PME estiment ne pas bénéficier d'un soutien adéquat en matière de cybersécurité.**

Ces entreprises font face à de nombreux défis tels que la limitation de ressources, de moyens, de connaissances et de sensibilisation aux risques de cybersécurité.

Il est essentiel de les accompagner de manière pragmatique et adaptée à leurs enjeux et à leurs ressources pour renforcer leur posture de sécurité.

Découvrir l'accompagnement Apave en cybersécurité pour les TPE PME

Avec une disparité selon l'effectif :



Partie 2/

Vous accompagner dans la maîtrise des risques cyber

1 Notre approche

Pour mieux se protéger contre les cyberattaques

La maîtrise des risques est un élément clé pour assurer la prévention des incidents et la sécurité des activités au sein d'une organisation. Pour cela, il est essentiel de prendre en compte trois facteurs de risques majeurs :

1 Humains

Les comportements, les compétences et les actions des individus au sein de l'organisation peuvent influencer la survenue d'incidents.

Ainsi, il est essentiel de :

- **Sensibiliser les employés** aux risques de cybersécurité et à leurs responsabilités.
- **Promouvoir une culture de sécurité** et encourager la vigilance, notamment avec des campagnes de phishing.

2 Organisationnels

La structure, les processus et la culture de l'organisation peuvent avoir un impact significatif sur la prévention des incidents.

Afin de minimiser ces risques organisationnels, il est nécessaire de mettre en place :

- Des **politiques et des procédures de sécurité** claires.
- Des **systèmes de gestion des risques** et de crises
- De **promouvoir la transparence et la communication** au sein de l'organisation.

3 Techniques

Les défaillances techniques et mes vulnérabilités informatiques sont autant de risques qui peuvent compromettre la sécurité des activités.

Pour réduire ces risques techniques, il est essentiel de :

- **Mettre en place des solutions de sécurité informatique** (pare-feu, antivirus, etc.).
- **Appliquer régulièrement les mises à jour** et les correctifs de sécurité
- **Systématiser l'évaluation cyber par la réalisation de diagnostics de cybersécurité**

En regroupant ces facteurs humains, organisationnels et techniques,
les TPE PME peuvent renforcer leur posture de cybersécurité et mieux se protéger contre les cyberattaques.

Découvrez notre accompagnement à la suite, dans notre fiche pratique !

apave

2 Fiche Pratique

Les étapes clés pour prévenir le risque de cyberattaque

Facteurs de risques :
- Humains
- Organisationnels
- Techniques

En se basant sur notre approche de **maîtrise des risques** et en prenant en compte les **besoins exprimés par les TPE et PME à travers cette enquête**, nous avons élaboré une **offre d'accompagnement spécifique.**

1. COMPRENDRE

- Résultats de l'enquête cyber adressée aux TPE PME
- Livre Blanc Dirigeant de TPE PME : mode d'emploi de votre cyberprotection
- Autodiagnostic cyber réalisable en moins de 5 minutes

2. EVALUER

- Diagnostic de cybersécurité
- Scan de vulnérabilité de vos sites web

3. FORMER

- Formation des collaborateurs en bonnes pratiques cyber
- Formation des managers aux enjeux de la cybersécurité

Toutes nos formations sont disponibles en e-Learning, présentiel ou classe virtuelle.

4. DEVELOPPER LA CULTURE

- Campagnes de phishing

5. STUCTURER L'ORGANISATION

- Mise en place de vos dispositifs : charte informatique, PSSI, PCA, PRA, gestion et communication de crise...

6. ALLER PLUS LOIN

- Certification cybersécurité ISO 27001

Découvrir l'offre Apave

Cliquez sur les liens soulignés pour en savoir plus sur nos offres !

3 Les bons réflexes à adopter

En cas de cyberattaque

1 Porter plainte dans les 72h

Auprès de la gendarmerie

2 Notifier l'incident à la CNIL dans les 72h

En cas de violation de données à caractère personnel

3 Contacter le dispositif d'assistance aux victimes

Avec le portail dédié : cybermalveillance.gouv.fr

4 Déclarer l'incident à votre assurance

Suivant les conditions de votre contrat

5 Déclarer l'incident à l'ANSSI si vous êtes :

- Un OIV (Opérateur d'Importance Vitale)
- Un OSE (Opérateur de Services Essentiels)
- Un FSN (Fournisseur de Service Numérique)

(Evolution à prévoir avec le NIS v2)

CONCLUSION

Aujourd'hui, les TPE et PME sont confrontées à des défis importants en matière de cybersécurité, avec des attaques réalisées par le biais des salariés représentant 70% des cas et entraînant des conséquences graves telles que l'arrêt des activités, les pertes financières et le vol de données. En tant que tiers de confiance numérique, nous comprenons parfaitement les enjeux auxquels vous êtes confrontés.

Bien que la prise de conscience progresse, de nombreuses entreprises manquent encore de ressources dédiées, de budgets spécifiques, de politiques de protection des données et de plans d'action. De nombreuses entreprises estiment ne pas être suffisamment accompagnées en matière de cybersécurité, justifiant en partie ces raisons.

Il est essentiel de renforcer l'accompagnement et le soutien offerts aux TPE et PME afin de renforcer leur sécurité et de faire face aux risques. En regroupant ces facteurs humains, organisationnels et techniques, les TPE et PME peuvent améliorer leur posture en matière de cybersécurité et se protéger de manière plus efficace contre les cyberattaques.

En tant qu'acteur majeur de la maîtrise des risques numériques, le groupe Apave se positionne à vos côtés pour vous accompagner dans votre démarche de prévention des risques cyber. Pour ce faire, nous avons développé une offre de maîtrise des risques numériques spécialement conçue pour répondre à vos besoins et attentes. Cette offre repose sur deux piliers fondamentaux : la cybersécurité et la protection des données, et elle est adaptée tant sur le plan technique qu'économique aux TPE, PME et collectivités.

Apave se distingue en tant que seul acteur "tiers de confiance numérique" à proposer cette approche globale, bénéficiant d'accréditations et de reconnaissances au niveau national et international.

Harold Huillier, Directeur Délégué du groupe Apave Digital

apave

Nos équipes sont mobilisées pour vous accompagner

MAÎTRISE DES RISQUES NUMÉRIQUES

01 76 34 05 36

contact-client@apave.com

france.apave.com