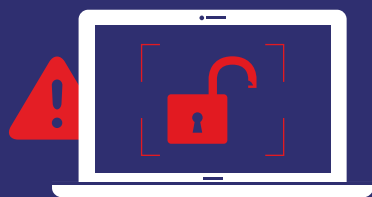


TPE/PME

L'ASSURANCE CYBER,

**Un partenaire essentiel
pour vous protéger**





49 % des entreprises ne sont toujours pas préparées aux cyberattaques¹.



La cybercriminalité constitue aujourd'hui un **risque majeur pour la continuité et la pérennité des entreprises**, en particulier pour les TPE et PME.

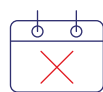


L'assurance cyber permet de vous protéger et de vous accompagner, en complément de vos dispositifs de cybersécurité techniques et organisationnels.

Les TPE et PME en première ligne du risque cyber



2/3 des cyberattaques ont ciblé des TPE et PME en 2025².



Un programme malveillant de type rançongiciel peut entraîner une interruption d'activité comprise entre **5 et 20 jours**, selon le niveau de cybersécurité de l'entreprise.



Pour une TPE/PME, le coût moyen d'une cyberattaque est estimé entre **30 000 et 600 000 euros**, soit 3 à 10 % du chiffre d'affaires annuel³.

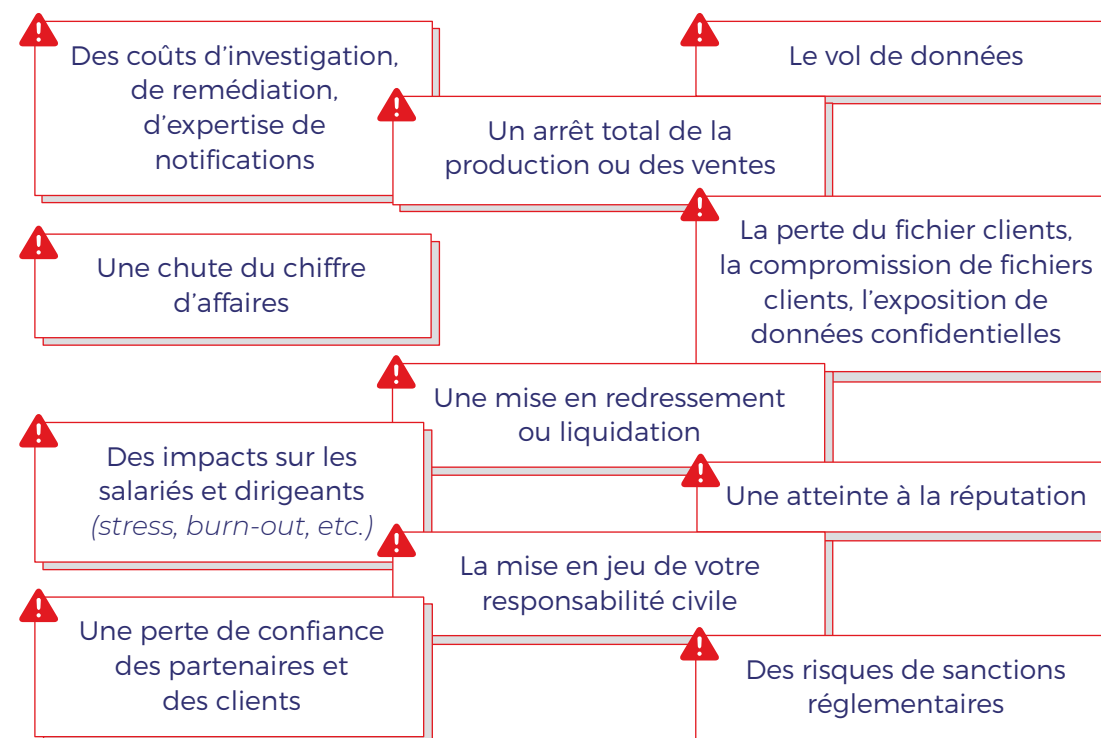
¹ 2^e édition du baromètre national de la maturité cyber des TPE-PME produit par cybermalveillance.gouv.fr en 2025

² Orange Cyberdefense, security Navigator 2026

³ Référence ANSSI 2024

Les conséquences réelles d'une cyberattaque

Une attaque peut entraîner :



Combien peut vous coûter une cyberattaque ?

Exemple pour une PME de 15 salariés, réalisant 3 millions d'euros de chiffre d'affaires



Intervention informatique d'urgence :
de 15 000 à 30 000 euros



Pertes d'exploitation :
de 20 000 à 100 000 euros



Honoraires juridiques :
de 5 000 à 25 000 euros



Communication de crise :
de 5 000 à 15 000 euros

Coût total potentiel

Entre 45 000 et plus de 170 000 euros

En l'absence d'assurance cyber, **100 % de ces coûts sont à la charge de l'entreprise.**

À quoi sert une assurance cyber ?

C'est un **contrat de couverture des risques cyber**, qui allie :

-  — des **actions de prévention proactive**
-  — des **dispositifs d'assistance et de gestion de crise**
-  — une **indemnisation financière** des préjudices subis

Elle permet :

En amont,

 de renforcer votre dispositif de prévention

En aval, en cas de cyberattaque,

 de vous accompagner dans la gestion de crise et de vous indemniser des conséquences financières de l'attaque

L'assurance cyber vous accompagne aussi en prévention

Comme le proposent aujourd'hui les principaux assureurs du marché, **l'assurance cyber ne se limite plus à indemniser après sinistre.**

Elle peut inclure

- un diagnostic initial de la maturité cyber
- des scans de vulnérabilité externes réguliers
- des recommandations techniques personnalisées
- des modules de sensibilisation des collaborateurs (*test de phishing, fraude au président...*)
- des formations e-learning sur la cybersécurité

 **Objectif**

Réduire votre exposition au risque en améliorant votre niveau de cybersécurité

Quelle est l'utilité d'une assurance cyber pour une TPE/PME ?

En cas de cyberattaque, vous êtes accompagné. Selon les garanties prévues au contrat, l'assurance cyber peut notamment :



Mettre à disposition une **assistance spécialisée 24h/24**



Mobiliser des **experts en réponse à incident**
(IT forensics, spécialistes, etc.)



Activer une **cellule de gestion de crise** (juridique, experts RGPD, communication)



Couvrir les **pertes d'exploitation** et les frais supplémentaires d'exploitation



Prendre en charge les **coûts d'investigation et de restauration des données et systèmes**



Couvrir les **frais juridiques et de défense**



Prendre en charge les **frais de la CNIL** en cas de fuite de données personnelles

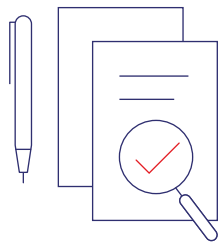


Couvrir les conséquences financières liées à la **responsabilité civile**

Les points clés à vérifier avant de souscrire une assurance cyber

Avant toute souscription, il est recommandé, avec l'accompagnement de son assureur ou de son intermédiaire, de porter une attention particulière aux points suivants :

- ✓ Les **plafonds de garantie** (*montant maximum d'intervention de l'assureur*)
- ✓ Les **franchises applicables** (*montant restant à votre charge*)
- ✓ Les **exclusions de garantie**
- ✓ La définition des **événements cyber couverts** (*origine malveillante et/ou accidentelle*)
- ✓ La couverture des **pertes d'exploitation** à la suite d'un événement cyber
- ✓ L'existence d'une **garantie de protection juridique dédiée**
- ✓ La prise en charge des **conséquences financières d'une cyber fraude** (*ex. : virement frauduleux, usurpation d'identité, etc.*)
- ✓ Les **délais de déclaration de sinistre**
- ✓ Les **obligations de cybersécurité** à respecter par l'entreprise (*sauvegardes régulières, mises à jour, etc.*)



Quels réflexes avoir en cas d'attaque cyber ?



Alertez immédiatement votre assureur au numéro d'urgence qui vous a été fourni lors de la souscription du contrat et votre support informatique.



Isolez les systèmes attaqués en coupant toutes les connexions à internet et au réseau local.



N'éteignez pas les systèmes concernés et préservez les preuves de l'attaque.



Ne payez pas de rançon.



En cas de cyberattaque, vous êtes tenu par la loi de déposer plainte dans un délai de 72 heures à partir de la découverte des pertes et dommages occasionnés par la cyberattaque.



Votre entreprise est tenue de notifier les violations de données personnelles à la CNIL dans un délai de 72 heures à la suite de la constatation de la violation.



Contactez votre assureur !



Conception graphique : Julien Tredan-Turini / www.julientredanturini.com



26 boulevard Haussmann
75009 Paris

franceassureurs.fr