Cybersécurité PME - Protéger l'essentiel, sans exploser son budget

La Cybersécurité à moindre coût pour les PME

CYBERID

19 MAI 2025

TABLE DES MATIERES

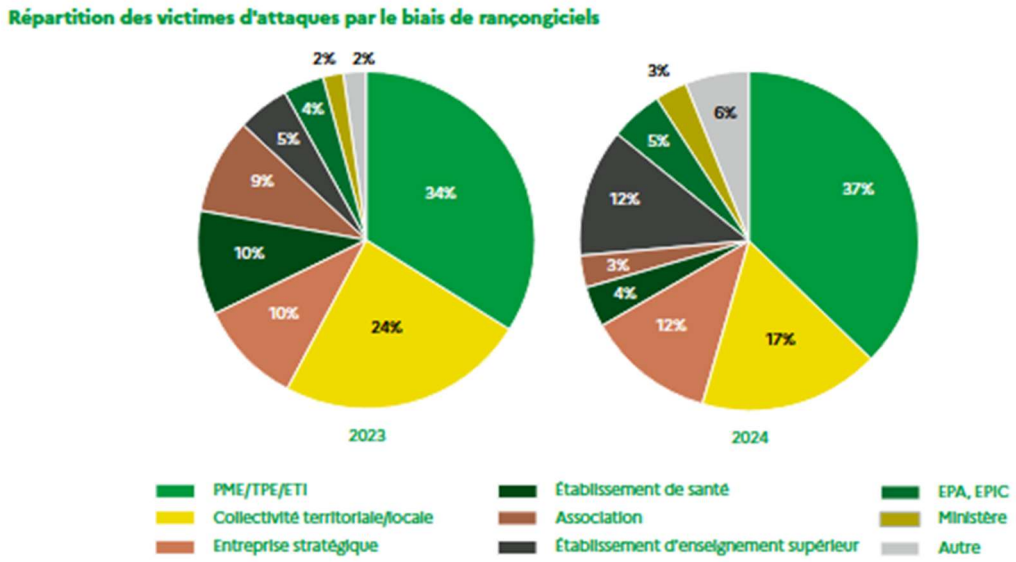
1. LA VISION

La cybersécurité : une responsabilité stratégique du dirigeant

Aujourd'hui, **les cybermenaces ne ciblent plus uniquement les grands groupes.** Ransomwares, hameçonnage, vol de données, sabotage : les PME sont devenues des cibles privilégiées, justement parce qu'elles sont perçues comme moins préparées.

Et pourtant, **plus d'une PME sur deux en France a déjà été confrontée à une attaque**, selon la CPME. Dans la majorité des cas, les conséquences ne sont pas seulement techniques : perte de données, interruption d'activité, dégradation de la réputation, voire dépôt de bilan.

La cybersécurité est désormais un sujet stratégique, qui relève directement de la direction. Comme pour la santé financière ou les obligations sociales, le dirigeant doit s'emparer du sujet. C'est lui qui doit **donner l'impulsion, fixer les règles, et rendre la sécurité compréhensible et applicable pour tous**.



Protéger l'essentiel sans complexité ni surcoût

Beaucoup de dirigeants pensent encore que la cybersécurité est trop complexe, trop technique ou trop chère pour leur entreprise. Cette doctrine prouve l'inverse : **on peut réduire efficacement les risques majeurs avec des gestes simples, peu coûteux et immédiatement applicables.**

Elle repose sur trois piliers fondamentaux :

- **Prioriser les actifs informationnels essentiels** : les boîtes mail, les fichiers clients, les outils comptables ou RH.
- **Adopter une hygiène numérique minimale** : des mots de passe robustes, des mises à jour régulières, des sauvegardes déconnectées, un Wi-Fi sécurisé, et des appareils mobiles protégés.
- **Instaurer une culture commune de la sécurité** : car **80 % des incidents viennent d'erreurs humaines**, pas de failles techniques.

📌 *La sécurité ne repose pas sur la technologie seule, mais sur des comportements clairs, répétés, compris et assumés à tous les niveaux de l'entreprise.*

Une doctrine pensée pour les PME, pas calquée sur les grands groupes

Plutôt que d'imiter les méthodes des grandes entreprises (souvent inadaptées aux PME), cette approche propose **un cadre souple, progressif, mais structuré**, spécifiquement conçu pour les petites structures, avec ou sans service informatique interne.

Elle permet à toute entreprise de :

- Identifier et protéger ses données critiques (analyse de risques simplifiée)
- Mettre en place des mesures concrètes et proportionnées
- Réagir efficacement en cas d'incident (grâce à un plan d'action d'urgence clair, incluant journal des incidents, contacts clés et consignes de dépôt de plainte — notamment en cas de ransomware, où **le paiement est à proscrire**)
- Se préparer à évoluer (RGPD, hébergement de données dans l'UE, appels d'offres)

🎯 *Protéger les données personnelles des clients et collaborateurs n'est pas une option : c'est une **obligation légale** (RGPD), même pour les plus petites structures.*

S'engager, c'est déjà se protéger

Ce livre blanc n'a pas vocation à transformer chaque PME en forteresse numérique. Il a pour ambition de **donner un cap simple, applicable et réaliste** à celles qui veulent avancer, en toute autonomie ou avec un accompagnement léger.

Vous n'avez pas besoin de tout comprendre, ni de tout faire dès demain. Mais vous devez **prendre la décision de ne plus ignorer le risque.**

💡 *La cybersécurité, c'est comme l'hygiène : on ne la remarque que lorsqu'elle manque.*

Commencez par les fondamentaux. Impliquez votre équipe. Tenez-vous informé.

Et surtout : **portez cette stratégie comme un pilier de la résilience de votre entreprise.**

2. PRINCIPES FONDAMENTAUX

Un socle de bon sens, pour des actions à fort impact

Dans un contexte où les cyberattaques se multiplient, **la sécurité numérique des PME ne peut plus reposer sur l'improvisation ou la chance.** Elle doit s'appuyer sur une approche claire, réaliste, et surtout adaptée aux moyens et aux réalités de terrain des petites structures.

Cette doctrine repose sur **cinq principes fondamentaux** qui permettent à toute PME, quel que soit son niveau de maturité technique, de **réduire efficacement son exposition aux risques les plus fréquents**.

1. La sécurité commence au sommet : le dirigeant est responsable

Le premier levier de sécurité, c'est la direction. Sans engagement clair du dirigeant, aucun outil ni aucune procédure ne sera véritablement appliqué.

📌 *L'ANSSI rappelle que la cybersécurité est une décision stratégique, pas une affaire purement technique.*

Cela signifie :

- Assumer la responsabilité de la sécurité de l'entreprise et de ses **actifs informationnels essentiels** (mails, données clients, comptabilité…)
- Intégrer la cybersécurité dans les arbitrages budgétaires et les priorités internes
- Montrer l'exemple et soutenir la montée en compétences des équipes

Un dirigeant engagé crée une culture où la vigilance devient naturelle.

2. Priorité à l'essentiel : 20 % d'effort, 80 % de protection

La perfection n'est pas atteignable ni nécessaire. L'objectif est de **protéger en priorité les points les plus critiques**, avec des mesures simples à fort effet levier.

Exemples de priorités :

- Accès aux comptes e-mail professionnels
- Sauvegardes des données critiques (clients, devis, RH…)
- Mise à jour régulière des logiciels et systèmes
- Protection des appareils mobiles utilisés pour le travail

🎯 *En cybersécurité, comme ailleurs, mieux vaut une protection simple mais bien appliquée qu'une stratégie complexe jamais mise en œuvre.*

3. Hygiène numérique avant sophistication technique

Dans l'esprit des recommandations de l'ANSSI, il est essentiel de développer une **hygiène numérique de base** dans toute l'entreprise.

Cela comprend :

- L'utilisation de **mots de passe robustes et uniques**
- L'activation systématique de la **double authentification**
- La **mise à jour automatique des logiciels, navigateurs, systèmes d'exploitation** et applications mobiles
- Le **verrouillage des smartphones et tablettes**, avec mot de passe ou biométrie, et prudence face aux applications inconnues
- La **désactivation ou séparation des réseaux Wi-Fi**, avec WPA2/WPA3, mot de passe fort, et un **réseau "invités"** distinct

Ce sont ces gestes simples et répétables qui font la différence au quotidien.

4. Responsabiliser les équipes, pas les techniciser

80 % des incidents de cybersécurité sont dus à une erreur humaine.
Il ne s'agit donc pas seulement d'installer les bons outils, mais de **sensibiliser tous les collaborateurs aux bons réflexes**.

Chaque employé peut :

- Identifier un e-mail suspect
- Refuser de transmettre des données sensibles par messagerie instantanée
- Respecter une politique de sécurité claire et compréhensible
- Savoir comment réagir et à qui signaler une anomalie

💡 *Une politique de sécurité en une page, intégrée au livret d'accueil ou affichée dans l'atelier, est souvent plus utile qu'un long document jamais lu.*

5. Construire une trajectoire, pas une forteresse

Cette doctrine ne vise pas l'exhaustivité, mais la **progressivité**. Chaque PME peut renforcer sa posture pas à pas, au fur et à mesure de sa croissance ou de ses contraintes clients.

Cela inclut :

- Une **analyse de risques simplifiée** (quelles données sont critiques ? quels incidents seraient les plus bloquants ?)
- La **mise en place de sauvegardes selon la règle des 3-2-1**, avec **déconnexion physique** du support hors ligne après chaque session
- L'existence d'un **plan d'action d'urgence** (PRA), même minimal, incluant un **journal des incidents**, les numéros à contacter, et la consigne de **ne jamais payer de rançon**, mais de **porter plainte immédiatement** (cf. cybermalveillance.gouv.fr)

Message-clé : la sécurité est une affaire de méthode, pas de moyens

Ce ne sont pas les PME qui sont vulnérables par nature. **Ce sont celles qui n'ont pas encore mis en place de principes simples, clairs et adaptés à leur taille.**

Prenez position. Impliquez vos équipes. Appliquez l'essentiel.
La cybersécurité peut devenir une force de votre entreprise.

3. OBJECTIFS STRATEGIQUES

Poser les bases d'une sécurité efficace, responsable et évolutive

La cybersécurité ne se résume pas à l'installation d'un antivirus ou à la mise en place de quelques mots de passe robustes. **C'est une stratégie à part entière**, pilotée par la direction, qui vise à protéger les actifs essentiels de l'entreprise, à maintenir la continuité d'activité, et à préparer l'avenir.

Cette doctrine repose sur **trois objectifs stratégiques** simples et réalistes, alignés avec les recommandations de l'ANSSI, pour aider les PME à renforcer leur résilience numérique **sans exploser leur budget, ni leur charge mentale.**

1. Réduire 80 % des risques avec 20 % des efforts

En appliquant les fondamentaux de l'**hygiène numérique**, une PME peut se protéger contre la majorité des attaques courantes.

Cela implique :

- Des **mots de passe solides et uniques**, centralisés dans un gestionnaire
- La **double authentification** activée sur les comptes critiques
- La **mise à jour automatique** des systèmes d'exploitation, logiciels métier, navigateurs et applications mobiles
- Le **verrouillage des appareils mobiles** (mot de passe, biométrie) et la vigilance face aux applications non vérifiées
- Un **Wi-Fi d'entreprise sécurisé**, avec cryptage WPA2 ou WPA3, mot de passe fort, et réseau invité séparé

Ces gestes simples ont un **effet démultiplicateur** sur la sécurité globale.

🎯 *Pas besoin de multiplier les outils : mieux vaut bien appliquer cinq règles essentielles que de mal gérer une solution sophistiquée.*

2. Donner aux PME une capacité de réaction autonome

Même sans service informatique interne, une PME doit pouvoir **réagir rapidement et efficacement en cas d'incident**.

Cela passe par :

- Un **Plan d'Action d'Urgence (PRA light)** clair, connu de tous, avec :
    - Qui appeler
    - Où sont les sauvegardes
    - Comment isoler un poste infecté

    - Que faire en cas de fuite de données
- L'inclusion d'un **journal des incidents** (date, cause probable, actions prises)
- La règle claire : **ne jamais payer de rançon** en cas d'attaque, mais **déposer plainte immédiatement** et alerter les autorités (via cybermalveillance.gouv.fr)

Ce socle permet d'agir vite, de limiter les dégâts et de rassurer clients, collaborateurs et partenaires.

3. Préparer l'entreprise à évoluer sans repartir de zéro

Une cybersécurité bien pensée aujourd'hui permet de **gagner en agilité demain** :

- En répondant à des appels d'offres publics ou grands comptes
- En se mettant en conformité avec le RGPD (traitement des données personnelles)
- En migrant vers des outils cloud européens avec une gestion des accès maîtrisée
- En conduisant une **analyse de risques simplifiée** : quels sont nos actifs critiques ? Quels scénarios d'incident sont les plus probables ?

Les fondations posées par cette doctrine peuvent ensuite être renforcées (audit externe, pare-feu professionnel, outils de supervision…) **sans tout reconstruire.**

📌 *La cybersécurité est un processus continu, pas un produit figé. Elle doit évoluer avec votre activité.*

Message-clé : Protéger aujourd'hui, construire pour demain

En adoptant cette doctrine, vous ne protégez pas seulement vos fichiers. Vous sécurisez votre activité, votre réputation et vos perspectives de croissance.

Et surtout : vous affirmez votre rôle de dirigeant responsable, engagé dans la protection de vos équipes, de vos clients, et de vos données.

4. PILIER 1 : HYGIENE NUMERIQUE MINIMALE (ZERO EURO)

La première ligne de défense : des gestes simples, gratuits et efficaces

Quand on parle de cybersécurité, on imagine souvent des outils complexes ou des budgets inaccessibles. En réalité, **80 % des risques peuvent être réduits par une meilleure hygiène numérique** — c'est-à-dire des habitudes simples, appliquées au quotidien par toute l'équipe.

Ce premier pilier montre qu'il est possible de protéger les **actifs informationnels essentiels** d'une PME sans dépenser un centime, simplement en renforçant les pratiques de base : mots de passe, mises à jour, accès, vigilance. C'est **le socle vital d'une entreprise résiliente**, recommandé aussi bien par l'ANSSI que par les plateformes publiques comme cybermalveillance.gouv.fr.

1. Des mots de passe robustes et bien gérés

Les mots de passe faibles, réutilisés ou partagés sont la porte d'entrée la plus fréquente des cyberattaques.

À mettre en place dès aujourd'hui :

- Un **gestionnaire de mots de passe gratuit** (Bitwarden, KeePass) pour générer et stocker des mots de passe uniques et complexes
- Une **politique claire** : aucun mot de passe ne doit être partagé ni stocké en clair (papier, e-mail, fichier non protégé)
- Un **mot de passe d'au moins 12 caractères**, mélangeant majuscules, chiffres et symboles

📌 *Le mot de passe est un élément critique. Il protège souvent l'ensemble des comptes d'une entreprise.*

2. La double authentification : indispensable sur les accès critiques

Activez la double authentification (2FA) **partout où c'est possible**, en priorité sur :

- Les boîtes mails professionnelles
- Les outils de gestion (facturation, CRM, comptabilité…)
- Les accès au cloud ou aux réseaux internes

Outils gratuits : Google Authenticator, Microsoft Authenticator, FreeOTP.

🎯 *Avec une 2FA activée, un mot de passe volé n'ouvre plus directement l'accès à vos données.*

3. Mettre à jour tous les logiciels, tout le temps

La gestion des mises à jour est un pilier central de l'hygiène numérique. Une faille non corrigée est une invitation ouverte aux attaquants.

À faire appliquer systématiquement :

- Activer les **mises à jour automatiques** sur les systèmes d'exploitation, navigateurs, logiciels métiers, antivirus
- Inclure les **applications mobiles utilisées à titre professionnel**
- Programmer une **vérification mensuelle** pour les appareils critiques

🔄 *Un logiciel non mis à jour, c'est comme une porte qu'on oublie de refermer.*

4. Sécuriser les appareils mobiles

Téléphones et tablettes sont devenus des outils de travail essentiels — mais aussi des points d'entrée sensibles.

Règles de base à faire respecter :

- **Verrouillage de l'écran** avec mot de passe, schéma, code ou biométrie
- **Applications vérifiées uniquement** (éviter les APK non officielles)
- **Sauvegarde chiffrée** si possible
- **Mises à jour régulières** comme pour les postes fixes
- Activation du **chiffrement des données** (disponible sur la plupart des appareils récents)

📱 *Un téléphone non protégé peut contenir autant d'informations critiques qu'un ordinateur.*

5. Sécuriser le Wi-Fi d'entreprise

Un Wi-Fi mal configuré, c'est une faille ouverte sur votre réseau interne.

Mesures simples à mettre en place :

- Utiliser un chiffrement **WPA2 ou WPA3** (à vérifier sur la box ou le routeur)
- Modifier le **mot de passe par défaut** et le changer régulièrement
- Créer un **réseau séparé pour les invités** ou les appareils non professionnels

💡 *Un mot de passe Wi-Fi partagé entre collaborateurs, visiteurs et appareils personnels multiplie les risques de contamination.*

6. Vigilance sur les canaux non sécurisés

Évitez d'envoyer ou de recevoir des données sensibles (RIB, mots de passe, contrats…) via :

- WhatsApp ou SMS
- E-mails non chiffrés

Préférez :

- Des plateformes de partage sécurisées (Cryptomator, Tresorit Send, SwissTransfer)
- Le chiffrement de bout en bout lorsqu'il est disponible

3. Une formation mensuelle de 1h = 80 % des erreurs évitées

Une cyberattaque par phishing ou par pièce jointe piégée peut souvent être évitée si l'employé est formé. Une sensibilisation régulière, courte et concrète suffit.

Thèmes à aborder :

- Reconnaître un e-mail frauduleux
- Sauvegarder ses fichiers
- Ne pas se connecter à un Wi-Fi public non sécurisé
- Utiliser un lien de partage sécurisé (plutôt qu'un envoi de fichier critique par WhatsApp)

Astuce : des ressources gratuites existent (kits de l'ANSSI, vidéos de sensibilisation en ligne).

4. Zéro partage de compte, zéro confusion

Partager un compte à plusieurs (ex. : même identifiant pour un logiciel ou une boîte e-mail) crée **un flou sur les responsabilités** et **multiplie les risques de fuite ou d'erreur**.

Recommandation :

- Créer un compte par utilisateur, même pour les outils gratuits.
- Désactiver les anciens comptes dès qu'un salarié quitte l'entreprise.

5. Pas d'information sensible par messagerie non sécurisée

Il est tentant de répondre rapidement à un client ou un collaborateur via WhatsApp ou e-mail. Mais certaines informations **ne doivent jamais transiter par des canaux non chiffrés** :

- Mot de passe
- RIB ou données bancaires
- Fichiers clients ou contrats confidentiels

Réflexe à adopter : utiliser une solution de partage chiffrée (CryptPad, Tresorit Send, Firefox Send) pour les documents sensibles.

Une défense numérique qui commence par le bon sens

Cette hygiène de base ne nécessite **ni budget, ni équipe technique**, mais simplement **de la clarté, des outils simples et de la discipline**.

Message-clé : La sécurité commence par la rigueur quotidienne

Vous n'avez pas besoin d'un expert ou d'un outil onéreux pour instaurer une véritable culture de cybersécurité dans votre entreprise.
Vous avez besoin d'engagement, de clarté, et d'une routine appliquée par tous.

👉 **Ce pilier est la brosse à dents de la cybersécurité : si chacun s'en sert correctement, les infections deviennent très rares.**

.

5. OUTILS GRATUITS ET TRES PEU COUTEUX

De bons outils existent. Et ils sont souvent gratuits.

Dans l'imaginaire collectif, sécuriser une entreprise implique de faire appel à des solutions techniques onéreuses, complexes à déployer, ou réservées aux grandes structures. En réalité, **de nombreux outils fiables, gratuits ou très abordables**, existent et sont **suffisants pour protéger les actifs informationnels essentiels** d'une PME lorsqu'ils sont bien choisis et bien configurés.

Le plus important n'est pas de multiplier les outils, mais de les **comprendre, les maîtriser, et les utiliser avec rigueur**. Cette sélection s'aligne sur les recommandations de l'ANSSI, tout en restant réaliste pour une petite structure.

1. Antivirus : efficace n'est pas forcément payant

Microsoft Defender, intégré gratuitement à Windows 10 et 11, offre un excellent niveau de protection pour les postes de travail, à condition d'être activé et mis à jour.

✅ Il propose :

- Une **protection en temps réel**
- Un **pare-feu intégré** configurable
- Une bonne intégration avec l'outil de mise à jour Windows Update

Pour les utilisateurs de Linux, l'outil open source **ClamAV** peut couvrir les besoins de base.

🔄 *Rappel : ne jamais installer deux antivirus sur un même poste. Cela crée des conflits et affaiblit la protection.*

2. Sauvegardes sécurisées : protéger les données vitales à moindre coût

La sauvegarde est votre filet de sécurité absolu.

Outils recommandés :

- **Duplicati** : open source, planifie des sauvegardes automatiques et chiffrées vers le cloud (Google Drive, Dropbox…)
- **BorgBackup** : robuste et automatisable, idéal pour les structures techniques
- **Cryptomator** : ajoute un chiffrement à vos fichiers stockés dans le cloud

💡 *Conformément à la règle ANSSI des 3-2-1, conservez toujours une **copie hors ligne (disque dur externe)**, **physiquement déconnectée** après chaque session.*

3. Pare-feu : simple et déjà intégré

Le **pare-feu Windows** est un outil puissant souvent sous-exploité. Il permet de :

- Filtrer les connexions entrantes et sortantes
- Limiter les applications ayant accès à Internet
- Activer un profil "réseau public" plus strict pour les postes nomades

Astuce : dans un environnement PME, interdire les connexions entrantes par défaut limite fortement les risques d'intrusion.

🛡️ *Un bon pare-feu est comme une serrure intelligente : il laisse passer uniquement ce qui est autorisé.*

4. Scanner de vulnérabilités : identifier ses failles

Un **scanner de vulnérabilités open source** comme **OpenVAS (Greenbone)** permet de détecter les failles sur vos systèmes (si vous avez un technicien ou prestataire pour l'exploiter).

En alternative, l'**ANSSI propose des kits d'auto-diagnostic** ou des démarches guidées via cybermalveillance.gouv.fr ou les CCI.

🔍 *Connaître ses failles, même basiquement, est une forme d'**analyse de risques simplifiée**, parfaitement adaptée aux PME.*

5. Sécuriser les accès internet et les appareils mobiles

Appareils mobiles :

- Installez une **application antivirus gratuite** (par exemple Bitdefender Mobile ou Sophos)
- Vérifiez que le **chiffrement est activé**
- Utilisez uniquement des **applications de sources fiables** (App Store, Google Play)

Wi-Fi entreprise :

- Activez **WPA2 ou WPA3**
- Changez les **identifiants d'administration de la box**
- Mettez en place un **réseau "invités" séparé**
- Interdisez les connexions automatiques aux réseaux publics sur les appareils professionnels

📱 *Un téléphone mal protégé peut contenir autant d'informations critiques qu'un ordinateur de bureau.*

6. Extensions et navigateurs sécurisés

Adoptez des navigateurs configurés pour la confidentialité :

- **Firefox** ou **Brave**, avec blocage intégré des traqueurs
- Extensions utiles :
    - **uBlock Origin** : bloqueur de pub et de scripts malveillants
    - **HTTPS Everywhere** : force les connexions sécurisées
    - **NoScript** (avancé) : contrôle des scripts JavaScript

7. Logiciels de sensibilisation et affichage interne

De nombreux **kits gratuits de sensibilisation** sont mis à disposition par l'ANSSI ou cybermalveillance.gouv.fr :

- Affiches à imprimer
- Quiz d'équipe
- Vidéos courtes et pédagogiques

🧠 *Ce sont des outils simples pour rappeler régulièrement les bons réflexes sans effort pédagogique.*

Message-clé : un bon outil, c'est un outil bien utilisé

La cybersécurité d'une PME repose moins sur le budget que sur la rigueur et la cohérence.
Ces outils gratuits ou très peu coûteux permettent de **poser les fondations d'une protection sérieuse**, surtout lorsqu'ils sont **pilotés par une direction impliquée**.

👉 **Commencez avec ces outils. Adoptez-les. Apprenez à les maîtriser. Et surtout, faites-en un réflexe partagé par toute l'équipe.**

.

6. SAUVEGARDES ET RECUPERATION

Sans sauvegarde, pas de continuité

Aucune entreprise n'est à l'abri d'un vol, d'un incendie, d'une erreur humaine ou d'une attaque par ransomware. Et pourtant, **près d'une PME sur deux n'a pas de stratégie de sauvegarde fiable**.

En cas de cyberincident, **les données sont souvent les premiers actifs informationnels essentiels à être compromis.** Or, sans sauvegarde, une PME peut perdre en quelques minutes des années de travail, de contacts clients ou de documents administratifs.

La bonne nouvelle : **il est possible de mettre en place une stratégie de sauvegarde efficace, fiable, et adaptée à une petite structure — sans budget conséquent.**

Appliquer la règle des 3-2-1

L'ANSSI recommande une approche simple et éprouvée, connue sous le nom de **règle des 3-2-1** :

- **3 copies de vos données** (1 originale + 2 copies)
- **2 types de supports différents** (par exemple disque dur + cloud)
- **1 copie hors ligne ou hors site**

Cela permet de faire face à tous les scénarios : vol, casse, ransomware, erreur de manipulation.

🔄 *Exemple concret :*

- L'original sur l'ordinateur
- Une sauvegarde automatique sur un cloud chiffré
- Une sauvegarde hebdomadaire sur un disque dur externe, **déconnecté physiquement après chaque session**

Les outils adaptés pour PME

Outils gratuits ou open source recommandés :

- **Duplicati** : sauvegardes chiffrées vers des services cloud, planifiables automatiquement
- **Cryptomator** : ajoute un chiffrement transparent à vos fichiers cloud
- **BorgBackup** : solution robuste pour les environnements plus techniques ou Linux

🧩 *Astuce : même un simple disque dur externe peut suffire si utilisé régulièrement et stocké en sécurité.*

Le rôle du dirigeant : poser la routine, exiger les preuves

Une stratégie de sauvegarde efficace n'est pas uniquement une affaire d'outils, mais **une décision de pilotage**. Le dirigeant doit s'assurer que les règles sont :

- **Claires** : qui sauvegarde quoi, quand, où ?
- **Suivies** : via un tableau ou un rapport de suivi
- **Testées** : une **restauration** doit être simulée au moins **tous les trimestres**

📌 *Une sauvegarde non testée est une fausse sécurité.*

Sauvegarder, c'est aussi se conformer au RGPD

La **protection des données personnelles** (clients, salariés, fournisseurs) n'est pas seulement une bonne pratique, c'est **une obligation légale** pour toutes les entreprises.

Une stratégie de sauvegarde permet :

- De **limiter la perte de données** en cas d'incident
- De **justifier ses efforts de protection** en cas de contrôle
- De répondre plus facilement aux demandes d'accès ou de suppression de données

🔐 *Une bonne politique de sauvegarde, c'est aussi un pas vers la conformité RGPD.*

Message-clé : la sauvegarde, c'est la résilience de votre entreprise

Investir du temps dans une stratégie de sauvegarde efficace, c'est vous assurer que votre entreprise peut continuer à fonctionner même après un incident. C'est aussi rassurer vos clients, vos partenaires, vos salariés.

👉 **Commencez petit : une copie, un réflexe, un test. Mais ne vous contentez pas d'espérer que tout ira bien.**

7. PLAN D'ACTION D'URGENCE (PRA LIGHT)

Ce n'est pas le chaos qui fait le plus de dégâts. C'est l'improvisation.

En cas d'attaque informatique, ce ne sont pas les outils techniques qui comptent d'abord, mais la **capacité à réagir rapidement, avec méthode et sang-froid**.

Pour une PME, un **Plan de Reprise d'Activité (PRA)** ne doit pas être un document complexe, oublié dans un tiroir. Il doit être un outil clair, concret, **utilisable immédiatement**, même sans service informatique.

L'objectif du **PRA light** est simple : savoir **quoi faire, qui appeler, et comment reprendre le contrôle**, pour éviter que l'incident ne devienne une crise.

Pourquoi le PRA est un outil stratégique pour le dirigeant

Un dirigeant de PME ne peut pas déléguer la gestion de crise en cas d'attaque. Il est le **pilote des décisions à prendre à chaud**, que ce soit pour prévenir les clients, coordonner les équipes ou relancer l'activité.

📌 *L'ANSSI recommande de formaliser un plan d'action d'urgence, même minimal, afin de préserver les actifs informationnels essentiels et limiter les impacts organisationnels.*

Un PRA light ne demande pas de moyens techniques. Il demande de **l'anticipation, de la clarté, et de la discipline**.

4 éléments essentiels d'un PRA light

1. Une fiche d'urgence papier + numérique

Elle doit être imprimée et accessible dans les locaux ou dans un classeur "Sécurité". Elle contient :

- Les **contacts à prévenir** (prestataire IT, gendarmerie numérique, assurance)
- La **procédure de déconnexion d'urgence** (débrancher un poste, couper le Wi-Fi)
- La **localisation des sauvegardes** (disque dur, cloud, contacts)
- La **liste des services critiques à restaurer en priorité**
- Une **règle claire** : **ne jamais payer de rançon**. En cas de ransomware, **déposer plainte immédiatement** et signaler l'incident sur cybermalveillance.gouv.fr

2. Un journal des incidents

Inspiré des recommandations de l'ANSSI, ce journal permet de :

- Documenter chaque incident (date, symptôme, décision prise, durée)
- Identifier les fragilités récurrentes
- Faciliter les échanges avec les autorités, les assurances ou les prestataires

🗒️ *Un journal bien tenu renforce la mémoire collective de l'entreprise face aux crises.*

3. Une répartition claire des rôles

Même dans une structure de 3 personnes, tout le monde doit savoir :

- Qui isole un poste infecté
- Qui alerte le prestataire
- Qui informe les clients si besoin
- Qui supervise la restauration des données

Cette répartition évite les blocages et les décisions contradictoires.

4. Une simulation par an

Comme une alarme incendie, **un test de PRA** permet de s'assurer que le plan est connu, compréhensible et activable rapidement. Cela peut prendre 30 minutes, une fois par an, mais c'est **un entraînement qui peut sauver l'activité**.

Penser aussi aux données personnelles (RGPD)

En cas de fuite de données (fichiers clients, bulletins de paie, RIB…), la PME est tenue de :

- Notifier la CNIL si nécessaire
- Informer les personnes concernées en cas de risque élevé
- Documenter les actions entreprises

Le PRA doit intégrer **une fiche "fuite de données"** pour anticiper cette situation : qui prévient ? quoi dire ? à qui s'adresser ?

🔐 *La transparence et la réactivité renforcent la confiance, même en cas d'incident.*

Message-clé : en cas d'incident, mieux vaut être prêt que parfait

Un bon PRA n'est pas celui qui coche toutes les cases.
C'est celui que l'on comprend, que l'on applique, et qui **évite de paniquer.**

👉 **Rédigez votre fiche, imprimez-la, testez-la une fois. Cela suffit à transformer un moment de chaos en un acte de gestion responsable.**

8. POLITIQUE DE SECURITE SIMPLIFIEE

Mieux vaut une page appliquée qu'un manuel ignoré

Dans les grandes entreprises, les politiques de sécurité font souvent des dizaines de pages… et personne ne les lit. Dans une PME, **l'enjeu est de faire simple, concret, et compris de tous**.

La politique de sécurité est **un document stratégique**, car il formalise les règles du jeu. C'est un outil de pilotage pour le dirigeant, **une boussole pour les collaborateurs**, et **une preuve d'engagement en cas d'audit, de litige ou d'incident**.

📌 *L'ANSSI recommande à toutes les structures, même les plus petites, de définir une politique claire autour de l'hygiène numérique, des responsabilités, et de la réaction aux incidents.*

Pourquoi chaque PME doit avoir sa politique

Une politique de sécurité bien conçue permet :

- De **clarifier les comportements attendus**
- D'**éduquer les nouveaux arrivants** et les prestataires
- D'éviter les confusions en cas d'incident
- De **structurer les responsabilités du dirigeant**, en tant que garant de la protection des actifs informationnels essentiels

Et ce, **même si l'entreprise n'a que 5 salariés**.

Une bonne politique tient sur une page

Elle doit être :

- **Simple** : phrases courtes, règles concrètes
- **Visuelle** : tableau ou liste à puces
- **Contextualisée** : adaptée à l'activité de l'entreprise

💡 *Exemples de rubriques à intégrer :*

1. Règles d'usage des outils numériques

- Ne jamais partager son mot de passe
- Toujours verrouiller son poste lorsqu'on s'absente
- Installer uniquement les logiciels autorisés
- Appliquer les mises à jour dès qu'elles sont proposées

2. Sécurisation des appareils mobiles

- Protéger son smartphone/tablette pro par un mot de passe ou une empreinte

- Ne pas installer d'applications non vérifiées
- Activer le chiffrement si disponible

3. Réseau et accès Wi-Fi

- Se connecter uniquement au Wi-Fi de l'entreprise ou au VPN
- Ne jamais utiliser un Wi-Fi public pour accéder à des données sensibles
- Séparer le Wi-Fi invité du réseau interne

4. Gestion des sauvegardes

- Vérifier que la sauvegarde est bien faite selon la procédure
- Ne jamais laisser un disque de sauvegarde branché en permanence
- Tester la restauration une fois par trimestre

5. Réaction aux incidents

- En cas de doute : prévenir immédiatement le référent ou le dirigeant
- Remplir une ligne dans le journal des incidents
- **Ne jamais payer une rançon** – suivre le protocole de dépôt de plainte

RGPD : un devoir légal, même pour les petites structures

Votre politique peut inclure une phrase type :

"L'entreprise s'engage à protéger les données personnelles de ses clients, salariés et partenaires, conformément au RGPD. Toute fuite ou perte de données doit être immédiatement signalée."

🔐 *Cette mention valorise votre professionnalisme et rassure vos interlocuteurs.*

Intégration et diffusion : la rendre vivante

- Ajouter la politique au **livret d'accueil**
- L'afficher dans un espace commun
- La relire collectivement lors d'un point trimestriel
- La signer par chaque salarié à son arrivée

Message-clé : des règles visibles et comprises valent mieux qu'un PDF oublié

Vous n'avez pas besoin d'un juriste ni d'un expert pour formaliser une politique de sécurité utile.
Vous avez besoin de bon sens, de clarté… et d'un document que vos équipes peuvent lire en 3 minutes.

👉 **Écrivez-la. Imprimez-la. Appliquez-la. Elle deviendra votre premier pare-feu humain.**

9. MONTEE EN MATURITE (FACULTATIF)

Aller plus loin, à son rythme

Une fois les bases posées — hygiène numérique, sauvegardes, plan d'urgence, politique claire — certaines PME souhaitent aller plus loin. Par ambition, par exigence client, ou parce que l'environnement réglementaire ou concurrentiel l'impose.

C'est ici que commence la **montée en maturité** : non pas un saut dans la complexité, mais une **progression maîtrisée**, pensée pour renforcer la sécurité de manière stratégique, conforme aux recommandations de l'ANSSI.

Pourquoi monter en maturité ?

Parce que la sécurité numérique ne se fige pas. Elle évolue avec :

- Le **développement de l'activité** (plus de clients, de données, de collaborateurs)
- L'entrée sur de **nouveaux marchés** (grands comptes, marchés publics, appels d'offres)
- La **mise en conformité avec le RGPD** ou des référentiels spécifiques (ISO 27001, HDS, etc.)
- Le **besoin de rassurer les partenaires** sur la fiabilité de votre système d'information

📈 *La cybersécurité devient un avantage concurrentiel quand elle est visible, assumée et structurée.*

Par où commencer ? Une progression réaliste en 4 étapes

1. Réaliser une analyse de risques simplifiée

L'objectif : identifier vos **actifs informationnels essentiels** (données critiques, outils clés, processus vitaux) et les menaces les plus probables.

Pas besoin d'un audit complexe : un tableau ou un atelier interne suffit pour :

- Classer les données par criticité
- Identifier les incidents les plus impactants
- Prioriser les protections à renforcer

🛠️ *L'ANSSI propose des grilles de réflexion accessibles pour les petites structures.*

2. Se mettre en conformité avec le RGPD

Même sans sous-traiter des données à grande échelle, toute PME doit :

- Tenir un **registre des traitements**
- Rédiger une **politique de confidentialité**
- Être capable de **répondre aux demandes des personnes concernées**

- Sécuriser les données par des **mesures proportionnées**

💡 *Cela peut commencer par une page dédiée sur votre site web, et une clause type dans vos contrats.*

3. Élever le niveau technique, progressivement

Une PME mature peut commencer à intégrer :

- Un **pare-feu matériel** ou une **solution de filtrage DNS**
- Un **EDR (Endpoint Detection and Response)** pour surveiller les comportements anormaux
- Une **gestion centralisée des mises à jour** et des accès
- Une **segmentation du réseau Wi-Fi** (administration / invités / production)

🎯 *Chaque outil technique doit être compris et utilisé, sinon il devient une illusion de sécurité.*

4. Se faire accompagner ou auditer

Sans aller vers un audit certifiant, il est possible de :

- Solliciter un **consultant indépendant** pour un diagnostic ciblé
- Utiliser les **ressources publiques** : CCI, Cybermalveillance.gouv.fr, cellules régionales ANSSI
- Bénéficier de **dispositifs de financement** à travers les chambres de commerce, France Num, ou les OPCO

Le rôle du dirigeant : piloter la maturité comme une évolution naturelle

Cette progression ne se délègue pas totalement. Elle demande au dirigeant :

- De fixer un **cap réaliste**
- D'intégrer la cybersécurité dans la stratégie d'entreprise
- De mobiliser l'équipe et les prestataires dans une **démarche continue**

🧭 *La sécurité n'est pas un état, c'est un mouvement. Et ce mouvement doit être initié au plus haut niveau.*

Message-clé : construire sur du solide, évoluer avec agilité

Vous n'avez pas besoin de tout faire maintenant.
Mais en posant des bases sérieuses, vous préparez votre entreprise à évoluer **sans reconstruire, sans paniquer, et sans retard stratégique.**

👉 **Pensez la cybersécurité comme un investissement progressif.**
C'est une assurance contre les imprévus… et un levier de crédibilité.

10. APPROCHE COMMUNAUTAIRE

La cybersécurité est plus forte quand elle est partagée

Dans un monde de menaces numériques en constante évolution, la **solitude est un facteur de vulnérabilité**. Trop de PME se croient isolées, pensent être « trop petites pour être concernées », ou peinent à comprendre par où commencer.

Pourtant, **d'autres entreprises autour d'elles vivent les mêmes enjeux** : protéger leurs fichiers clients, éviter un blocage de leur activité, ou répondre à une demande de conformité.

L'approche communautaire, fortement encouragée par l'ANSSI, repose sur un principe simple : **mutualiser les connaissances, les outils et les bonnes pratiques pour progresser collectivement**.

🤝 *La sécurité numérique ne doit pas être un sujet réservé aux experts. Elle devient plus accessible, plus efficace et plus humaine lorsqu'elle est partagée.*

Pourquoi favoriser une dynamique collective ?

- Pour **ne pas réinventer la roue à chaque fois**
- Pour **accéder à des retours d'expérience concrets**
- Pour **être alerté rapidement en cas de menace locale ou sectorielle**
- Pour **renforcer la culture numérique au sein de son écosystème**

Un dirigeant qui s'engage dans cette démarche communautaire **n'élève pas seulement sa propre entreprise**, il **contribue à sécuriser un tissu économique tout entier**.

Comment mettre en place une approche communautaire ?

1. Créer ou rejoindre un groupe local d'échange

- Un groupe WhatsApp, Signal ou un mailing liste avec d'autres dirigeants ou responsables de TPE/PME
- Des réunions trimestrielles dans des tiers-lieux, via une CCI ou une fédération professionnelle
- Un canal de veille sur les **mises à jour critiques, les incidents récents ou les bonnes pratiques à partager**

💡 *Exemple : une entreprise peut alerter les autres sur une vague de phishing sectorielle, évitant ainsi une généralisation de l'incident.*

2. Organiser des ateliers ou simulations collaboratives

- Test de restauration de sauvegarde entre pairs
- Atelier "rédige ton PRA light" en une heure

- Présentation d'un outil gratuit par un autre entrepreneur

🧠 *Cela permet à chacun de progresser sans pression, dans un cadre bienveillant et applicable.*

3. Mutualiser certaines ressources

- **Modèles de politique de sécurité**, fiches PRA, affiches de sensibilisation
- Achat groupé de formations, d'outils ou de services ponctuels
- Recommandation de **prestataires locaux de confiance**

4. Valoriser la démarche

- Créer un **label local ou un badge d'engagement** (« PME cyber vigilante »)
- Mentionner sur son site ou dans sa signature mail que l'entreprise applique les recommandations ANSSI ou participe à un réseau d'échange
- **Impliquer ses partenaires, sous-traitants et fournisseurs** dans cette dynamique

Une culture de responsabilité, pas de surveillance

L'approche communautaire ne vise pas à fliquer ou à standardiser. Elle vise à créer **une culture partagée de la vigilance, de la responsabilité et du progrès collectif**, alignée avec les principes d'hygiène numérique, de protection des données personnelles (RGPD), et de gestion des risques proportionnée.

📌 *Une PME qui forme ses équipes, partage ses outils et documente ses incidents (via un journal simplifié), devient une actrice de la sécurité collective.*

Ressources utiles pour animer votre réseau

- www.cybermalveillance.gouv.fr : kits de sensibilisation, fiches pratiques, outils gratuits
- www.ssi.gouv.fr (ANSSI) : guides d'hygiène informatique, référentiels, conseils pour dirigeants
- Chambres de commerce, réseaux d'entrepreneurs, pôles territoriaux de cybersécurité

Message-clé : la cybersécurité, c'est un sport d'équipe

Il n'y a pas de concurrence sur la sécurité. Il n'y a que des alliés.

👉 **Faites le premier pas : partagez un bon réflexe, une astuce, ou un modèle de fiche avec une autre entreprise. Créez un groupe, organisez un café cyber. Vous serez surpris de voir à quel point les autres en ont aussi besoin.**