



CYBERSÉCURITÉ **POURQUOI SAVOIR** **NE SUFFIT PAS À AGIR**

**Décryptage des 12 tendances
remarquables de 2026**

[LA BOÎTE À MOTS]
AGENCE DE PLANNING ÉDITORIAL & SOCIÉTÉ À MISSION

[La boîte à mots] est une entreprise labellisée par Urgence Cyber région Sud pour ses activités de sensibilisation à la cybersécurité et de communication de crise.



SOMMAIRE

Préface — Antoine Parmentier, Urgence Cyber région Sud	3
Introduction — Savoir ne suffit pas à agir	4
LES 12 TENDANCES	
01. Les années 2025-2026 : un tournant dans la prise de conscience de la menace cyber	6
02. Il y a un décalage, souvent très net, entre la conscience du risque cyber et la maturité “opérationnelle” des entreprises	8
03. Plus l’organisation est grande, plus le risque cyber est perçu comme grand... mais plus on se sent paradoxalement protégé (la gestion du risque relevant « des autres »)	10
04. Les attaques d’opportunité sont largement sous-estimées par les petites structures qui, de ce fait, ne se perçoivent pas comme des cibles intéressantes	12
05. L’évaluation du risque cyber est souvent victime d’une illusion de rationalité stratégique	14
06. Les petites structures surestiment l’effort nécessaire pour agir (et ont tendance à procrastiner)	16
07. De manière générale, on privilégie en première intention les petites mesures visibles et ponctuelles plutôt que les fondamentaux continus	18
08. La technicité du risque cyber occulte sa dimension de gouvernance	20
09. Chez les TPE/PME, il existe une dépendance forte à des prestataires externes (infogérant, agences web, éditeurs de logiciels métiers)	22
10. Facteur humain : on se considère rarement comme étant le maillon faible	24
11. La montée en puissance du shadow IT	26
12. La maturité cyber est intrinsèquement liée à l’écosystème de l’organisation	28

[La boîte à mots]

Agence de planning éditorial

Société à mission

Directrice de la publication :

Emilie TRANCHANT

www.laboiteamots.fr

19/10/2026 ©2026 [La boîte à mots].

Tous droits réservés

Préface



**Antoine
PARMENTIER**

*Responsable de la cellule
de réponse à incident
régionale,
Urgence Cyber région Sud*

Depuis la création d'Urgence Cyber région Sud, les entreprises, collectivités et associations que nous accompagnons nous donnent à voir des réalités très différentes face au risque cyber.

Nous rencontrons des organisations particulièrement matures, qui ont intégré depuis plusieurs années la cybersécurité à leur fonctionnement. Elles ont identifié leurs vulnérabilités, structuré leurs procédures, sensibilisé leurs collaborateurs et, pour certaines, se préparent régulièrement à la gestion d'un incident.

Mais nous rencontrons en majorité des structures qui restent très peu préparées. Certaines découvrent au moment de l'incident l'étendue de leurs dépendances numériques, l'importance d'une sauvegarde réellement exploitable, la nécessité d'avoir identifié les bons interlocuteurs ou, tout simplement, les conséquences très concrètes que peut avoir une attaque sur la poursuite de leur activité.

Entre ces deux extrêmes, la réalité est faite d'une multitude de situations intermédiaires. D'autant plus que prise de conscience et préparation ne vont pas nécessairement de pair. Répéter les bonnes pratiques est indispensable, mais ne suffit pas toujours à provoquer le passage à l'action. Pour faire progresser durablement la maturité cyber, nous devons également mieux comprendre ce qui favorise l'adoption d'une mesure, ce qui la retarde, ce qui suscite de la résistance ou, au contraire, ce qui permet à une organisation de s'en saisir.

C'est tout l'intérêt du travail proposé par [La Boîte à Mots], entreprise labellisée par Urgence Cyber région Sud. En confrontant les tendances observées aux mécanismes humains, psychosociaux et organisationnels susceptibles de les expliquer, cette publication apporte un éclairage complémentaire à notre propre retour d'expérience.

Pour un CSIRT territorial, cette compréhension est loin d'être théorique. Elle doit nous aider à mieux sensibiliser, mieux orienter et mieux accompagner les organisations en tenant compte de leur réalité, de leurs contraintes et de leur niveau de maturité.

SAVOIR NE SUFFIT PAS A AGIR

En matière de cybersécurité, nous avons souvent tendance à imaginer le changement comme un processus relativement linéaire : réaliser un diagnostic, identifier les vulnérabilités, sensibiliser, recommander des mesures correctives et attendre que l'organisation les mette en œuvre. Comme si savoir ce qu'il fallait faire suffisait à déclencher l'action.

Or c'est précisément dans l'espace qui sépare la prise de conscience du passage à l'acte que se joue une grande partie de la maturité cyber des organisations. Une transition cyber ne consiste pas simplement à ajouter quelques outils ou quelques bonnes pratiques à un fonctionnement existant ; elle suppose parfois de renoncer à des habitudes, de modifier des arbitrages, de redistribuer des responsabilités ou d'accepter de nouvelles contraintes. Elle peut toucher aux usages quotidiens, aux processus, à la gouvernance, aux relations avec les prestataires, aux investissements et parfois à l'organisation même du travail. Il faut donc prendre la mesure de la transformation demandée, mais aussi de l'incertitude et des résistances qu'elle peut générer.

C'est particulièrement visible dans les petites structures. Le dirigeant d'une TPE ou d'une PME sait souvent qu'un incident grave pourrait menacer directement la continuité de son activité. Mais il doit simultanément gérer la trésorerie, les clients, le recrutement, la production et toutes les urgences du quotidien. Lui présenter une nouvelle liste de vulnérabilités, de procédures et d'investissements nécessaires peut alors produire l'effet inverse de celui recherché : plus le chantier paraît vaste, plus le premier pas devient difficile à faire.

Dans les grandes organisations, les mécanismes sont différents. Les moyens existent davantage, les responsabilités sont formalisées et la cybersécurité est souvent portée par des équipes spécialisées. Mais cette organisation peut elle-même créer une distance avec le risque. Parce que « quelqu'un s'en occupe », chacun peut sous-estimer sa propre responsabilité. Et lorsque survient une crise, la majorité des collaborateurs n'en voit souvent que le début et la fin : un service devient indisponible, puis revient. Tout le travail nécessaire au rétablissement reste invisible. Plus l'organisation est capable d'absorber le choc, plus elle peut paradoxalement donner l'impression que le système se répare presque tout seul.

Dans tous ces cas pratiques, savoir ne suffit pas.

C'est pourquoi, à travers les tendances observées en 2025-2026, nous avons choisi, pour ce Mois de la cyber, de déplacer la focale. Plutôt que de nous intéresser uniquement aux vulnérabilités et aux mesures de protection, nous avons cherché à comprendre ce qui se joue derrière les comportements et les situations auxquels sont confrontés les acteurs de la cybersécurité.

Car derrière une vulnérabilité qui perdure sont aussi à l'œuvre des mécanismes humains, psychosociaux et organisationnels : perception du risque, sentiment de vulnérabilité, charge mentale, biais cognitifs, dilution de la responsabilité, sentiment de protection, rapport au coût, complexité perçue ou encore normes collectives.

Ces mécanismes ne sont pas accessoires. Ils contribuent à expliquer pourquoi des organisations pourtant informées, sensibilisées et parfois même correctement équipées peinent encore à faire évoluer leurs pratiques.

TENDANCE N°1

Les années 2025-26 ont marqué un tournant dans la prise de conscience de la menace cyber par les entreprises

Ce que l'on constate

Les années 2025-2026 semblent marquer une évolution dans la manière dont les TPE et PME appréhendent le risque cyber. Là où la cybersécurité pouvait encore être considérée comme un sujet technique réservé aux grandes organisations, elle s'installe progressivement parmi les préoccupations concrètes des entreprises. Les incidents se rapprochent : une entreprise du même secteur paralysée, un fournisseur compromis, un client victime d'une fuite de données, une collectivité ou un établissement de santé du territoire touché par une attaque. À mesure que ces situations deviennent plus visibles et plus proches, le risque cesse d'être seulement théorique pour s'inscrire dans l'environnement quotidien des organisations.

Cette évolution ne signifie pas pour autant que toutes les entreprises ont atteint le même niveau de maturité, ni que cette prise de conscience se traduit systématiquement par des mesures de protection. Elle révèle plutôt **un changement progressif de représentation du risque**. La question « pourquoi nous attaquerait-on ? », encore très présente notamment dans les petites structures, commence à coexister avec une autre interrogation : « que se passerait-il si cela nous arrivait ? ». Et, progressivement, avec une troisième : « **sommes-nous réellement prêts ?** ». C'est sans doute là que se situe le changement le plus significatif : le risque cyber commence à être envisagé non plus seulement à travers la probabilité d'être attaqué, mais à travers la capacité de l'organisation à absorber l'incident et à poursuivre son activité.

Les chiffres à l'appui

- ➔ 44 % des entreprises interrogées estiment être fortement exposées au risque cyber, contre 38 % en 2024, soit +6 points.¹
- ➔ 15 % envisagent d'augmenter leur budget cybersécurité, soit 5 points de plus que l'année précédente.¹
- ➔ Plus de 50 % des entreprises interrogées estiment que la menace d'origine étatique est en augmentation.²
- ➔ 40 % considèrent le cyberespionnage comme un risque élevé.²
- ➔ Plus d'une entreprise sur deux se déclare concernée par les enjeux de souveraineté numérique et de cloud de confiance.²

¹ - Source : [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) / OpinionWay, [2e baromètre national de la maturité cyber des TPE-PME](#), octobre 2025. Enquête auprès de 588 entreprises de moins de 250 salariés.

² - Le baromètre [CESIN / OpinionWay](#) (janvier 2026) porte sur la cybersécurité des organisations françaises. Sa 11e édition repose sur les réponses de 397 RSSI et directeurs de la cybersécurité.

Analyse des mécanismes en jeu

Deux dynamiques principales expliquent ce tournant.

La première tient à l'évolution de la conflictualité internationale. Le cyber est désormais identifié comme un outil de guerre à part entière. Les tensions géopolitiques, la multiplication des opérations hybrides et la circulation d'outils offensifs issus d'acteurs étatiques contribuent à banaliser l'idée que le cyber est un champ de confrontation permanent. Même sans être une cible stratégique, une entreprise peut devenir une victime collatérale d'attaques plus larges.

La seconde, qui est liée, est la médiatisation accrue des incidents. Les attaques ne sont plus traitées comme des faits divers techniques, mais comme des événements économiques et stratégiques. Les blocages d'hôpitaux, les paralysies d'entreprises industrielles, ou les fuites massives de données sont largement relayés. Cette visibilité rend le risque plus saillant et plus crédible.

Cette double dynamique a transformé la perception du risque ces dernières années ; la menace y devient systémique.



TENDANCE N°2

Il y a un décalage, souvent très net, entre la conscience du risque cyber et la maturité “opérationnelle” des entreprises

Ce que l'on constate

La cybersécurité a incontestablement gagné en visibilité. Les professionnels sont aujourd'hui beaucoup plus familiers avec le vocabulaire du risque : rançongiciel, hameçonnage, vol de données, usurpation d'identité ou encore double authentification sont désormais des notions largement diffusées. La nécessité de se protéger est elle aussi beaucoup moins contestée. Pour autant, cette progression de la connaissance générale du risque ne se traduit pas automatiquement par une maturité opérationnelle équivalente.

Dès que l'on quitte le registre de la sensibilisation pour descendre au niveau des pratiques concrètes, des écarts importants apparaissent : connaissance précise des actifs et des accès, politique de mises à jour, déploiement du MFA, gestion des mots de passe, sauvegardes régulières et surtout testées, procédures en cas d'incident, segmentation des systèmes, journalisation ou encore préparation à la reprise d'activité. Autrement dit, **savoir que le risque existe ne signifie ni savoir précisément où l'organisation est vulnérable, ni avoir organisé sa capacité à réagir lorsqu'un incident survient.**

Ce décalage est particulièrement visible dans les TPE et PME. La cybersécurité entre en concurrence avec des préoccupations beaucoup plus immédiates : trésorerie, activité commerciale, recrutement, production, relation client ou simplement gestion quotidienne de l'entreprise. Le sujet n'est donc pas nécessairement ignoré ; il est souvent repoussé ou traité par touches successives, au gré des urgences, des recommandations d'un prestataire ou d'un incident.

Il en résulte une situation paradoxale : les organisations peuvent avoir considérablement progressé dans leur perception du risque sans avoir progressé dans les mêmes proportions dans leur capacité à y faire face.

Les chiffres à l'appui

- ➔ 52 % des TPE-PME craignent de perdre ou de se faire pirater leurs données, mais seulement 32 % disposent d'une authentification multifacteur.³
- ➔ **58 % des TPE-PME françaises estiment bénéficier d'un bon ou très bon niveau de protection. Pourtant, 80 % reconnaissent ne pas être préparées à une cyberattaque ou ignorent si elles le sont.**⁴
- ➔ 84 % disposent d'un antivirus, mais seulement 46 % utilisent un gestionnaire de mots de passe et 26 % une solution de double authentification.⁴
- ➔ Seulement 24 % des TPE-PME déclarent disposer d'une procédure de réaction en cas de cyberattaque.⁴

³ - Source : France Num / Crédoc / Direction générale des Entreprises, [Baromètre France Num 2025](#)

⁴ - Source : Cybermalveillance.gouv.fr / OpinionWay, [2e baromètre national de la maturité cyber des TPE-PME](#), octobre 2025. Enquête auprès de 588 entreprises de moins de 250 salariés.

Analyse des mécanismes en jeu

Dire que « la menace cyber augmente » est aujourd'hui un énoncé socialement attendu au même titre que dire « la transition écologique est un enjeu majeur » ; mais cet énoncé relève davantage du lieu commun que du registre opératoire.

En pratique, la menace cyber représente une "inconnue" qui entraîne des mécanismes de dissonance cognitive. Pour la réduire, plusieurs stratégies inconscientes peuvent être mobilisées, telles que :

- les petites tâches accumulées (le biais d'action comme on le verra plus loin)
- la minimisation implicite ou le déni (« nous sommes trop petits pour être ciblés »),
- le déplacement temporel (« on s'en occupera plus tard »),
- la relativisation (« on a déjà un antivirus »)
- ou le déplacement de priorité (« aujourd'hui, la trésorerie est plus urgente »)

Dans certains cas, la déclaration publique (« la menace augmente ») peut être une compensation symbolique de l'inaction pratique.



TENDANCE N°3

Plus l'organisation est grande, plus le risque cyber est perçu comme grand... mais plus on se sent paradoxalement protégé (la gestion du risque relevant « des autres »)

Ce que l'on constate

De manière contradictoire, plus une organisation est grande, plus elle se perçoit simultanément comme une cible ET comme un acteur protégé. Cette double perception repose sur des mécanismes en apparence opposés mais compatibles dans les faits.

Les grandes organisations savent qu'elles concentrent des actifs critiques : données, flux financiers, fonctions vitales, exposition médiatique. Elles sont plus souvent sensibilisées aux discours sur la menace, reçoivent davantage d'alertes (prestataires, autorités, assureurs) et disposent parfois d'un historique d'incidents plus riche. Cette accumulation produit une conscience aiguë de l'attractivité comme cible.

Très concrètement, on ne se sent pas menacé parce qu'on est fragile, mais parce qu'on est important.

Et paradoxalement cette même taille génère un sentiment de protection structurelle. Ressources financières, équipes dédiées, contrats avec des prestataires, assurances, procédures formelles, proximité perçue avec les autorités : tout cela alimente une croyance en une capacité supérieure à encaisser le choc.

Les chiffres à l'appui

- ➔ **45 % des ETI se considèrent vulnérables aux cybermenaces⁵**
- ➔ **Mais : dans une autre étude 83 % des dirigeants interrogés à l'international se déclarent préparés à faire face aux cybermenaces.⁶**
- ➔ A contrario : 29 % seulement des PME se considèrent vulnérables aux cybermenaces ⁵
- ➔ Et 15 % des TPE.⁵

⁵ -Docaposte / Cyblex Consulting, [Baromètre de la cybersécurité 2025](#), 3e édition, publié le 11 février 2026. Enquête réalisée auprès de 518 décideurs français.

⁶ - Beazley, [Spotlight on Tech Transformation & Cyber Risk 2025](#), enquête Risk & Resilience 2025-2026.

Analyse des mécanismes en jeu

Dans les grandes structures, la menace cyber est généralement bien identifiée, notamment au niveau des directions. Mais cette prise en compte peut paradoxalement renforcer le sentiment que le risque est déjà « traité quelque part ». Équipes dédiées, RSSI, prestataires, procédures, plans de continuité : l'existence même de ces dispositifs crée une forme de réassurance. **La cybersécurité apparaît comme une fonction spécialisée dont d'autres ont la charge (biais de délégation).**

Ce sentiment peut être renforcé par l'expérience des incidents eux-mêmes. Dans une grande organisation, la majorité des collaborateurs ne participe pas directement à la gestion d'une crise cyber. Ils en perçoivent les manifestations — un outil indisponible, des accès suspendus, de nouvelles consignes — puis constatent, quelques heures ou quelques jours plus tard, le retour à la normale. Entre les deux, tout le travail nécessaire à la résolution de la crise reste largement invisible : mobilisation des équipes, investigation, restauration des systèmes, arbitrages, solutions de contournement, coûts financiers ou humains.

Le retour à la normale peut ainsi donner l'illusion que la crise s'est, en quelque sorte, résolue d'elle-même. Et plus l'organisation est efficace pour absorber le choc, plus cet effort de résilience peut passer inaperçu aux yeux de ceux qui en bénéficient. Le succès du dispositif nourrit alors paradoxalement un sentiment de sécurité : « il y a eu un incident, mais finalement tout est rentré dans l'ordre ». C'est un effet de réassurance institutionnelle, qui induit un biais d'optimisme.



TENDANCE N°4

Les attaques d'opportunité sont largement sous-estimées par les petites structures qui, de ce fait, ne se perçoivent pas comme des cibles intéressantes

Ce que l'on constate

Les petites structures ont encore tendance à considérer qu'elles ne constituent pas des cibles suffisamment attractives pour les cybercriminels. Leur raisonnement repose souvent sur leur taille, un chiffre d'affaires modeste, une faible notoriété ou l'idée qu'elles ne détiennent pas de données présentant une valeur stratégique particulière. Dans cette représentation, une cyberattaque suppose un attaquant qui choisit délibérément sa victime : les grandes entreprises, les administrations, les infrastructures critiques ou les organisations détenant des informations sensibles seraient donc naturellement plus exposées.

Cette perception entretient une confusion importante entre être ciblé et être exposé. Une entreprise peut en effet ne présenter aucun intérêt stratégique particulier et se trouver néanmoins sur le chemin d'une campagne d'attaque. Une simple adresse électronique peut suffire à la faire entrer dans le champ d'action d'un attaquant.

Une part importante de la cybercriminalité repose en effet sur des logiques opportunistes et industrialisées. Campagnes massives de phishing, scans automatisés de vulnérabilités, tentatives d'authentification à partir d'identifiants compromis ou exploitation de failles connues permettent de tester simultanément un très grand nombre d'organisations. **L'attaquant ne cherche alors pas nécessairement une entreprise particulière : il cherche une vulnérabilité exploitable.** La logique économique est pragmatique : identifier les points d'entrée les moins coûteux à exploiter pour déployer un rançongiciel, détourner un compte, revendre un accès ou exfiltrer des données monétisables.

Dans ce contexte, la petite taille ne constitue pas nécessairement une protection. Elle peut même devenir un facteur de vulnérabilité lorsque des moyens plus limités conduisent à des systèmes moins surveillés, des mises à jour différées ou des accès insuffisamment sécurisés.

Les chiffres à l'appui

- ➔ **64 % des petites entreprises interrogées ne pensent pas constituer des cibles attractives pour les cybercriminels. Pourtant, 79 % déclarent avoir subi au moins un incident cyber au cours des cinq dernières années.**⁷
- ➔ 38 % des compromissions étudiées concernant les PME sont associées à l'utilisation d'identifiants compromis et 29 % à l'exploitation de vulnérabilités non corrigées sur des équipements exposés.⁸
- ➔ Environ 96 % des victimes de rançongiciels dont la taille est connue dans l'échantillon étudié sont des PME.⁸

⁷ Source : [Coalition, Small Business Cybersecurity Study](#), 2025 — enquête internationale auprès de 1 000 petites entreprises.

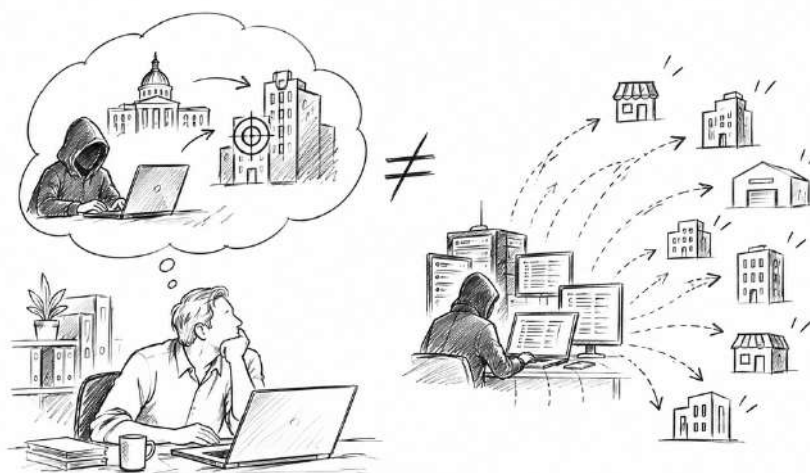
⁸ Source : Verizon, [Data Breach Investigations Report](#) 2026, section « Small- and Medium-Sized Businesses », p. 98

Analyse des mécanismes en jeu

Il ne s'agit pas ici d'un mécanisme de déni mais plutôt d'une méconnaissance des logiques économiques et techniques du cybercrime. Beaucoup d'entrepreneurs imaginent encore la menace sous une forme spectaculaire : attaque étatique sophistiquée, hacker isolé et expert ciblant une organisation spécifique. Cette représentation fantasmée – l'État hostile, le « hacker à capuche » – masque la réalité dominante : des infrastructures criminelles industrialisées, fonctionnant par automatisation et recherche de rendement.

Les attaquants raisonnent en termes de coût d'effort minimal et de retour sur investissement maximal. Ils n'ont pas besoin que l'entreprise soit « intéressante » ; ils ont besoin qu'elle soit accessible.

Cette incompréhension du mode opératoire conduit à une sous-évaluation du risque réel. Tant que l'entreprise pense qu'il faut être stratégique pour être attaqué, elle ne perçoit pas qu'il suffit d'être vulnérable pour l'être.



TENDANCE N°5

L'évaluation du risque cyber est souvent victime d'une illusion de rationalité stratégique

Ce que l'on constate

De nombreux acteurs expliquent leur niveau d'investissement en cybersécurité par un raisonnement présenté comme rationnel : arbitrage budgétaire, priorisation des risques, optimisation de ressources nécessairement limitées. Dans un environnement où les investissements possibles sont nombreux et les moyens contraints, la décision de ne pas investir davantage dans la cybersécurité apparaît alors comme le résultat d'un calcul implicite de rapport coût/bénéfice : pourquoi engager aujourd'hui des dépenses certaines pour se prémunir contre un événement dont la survenue demeure hypothétique ?

Le raisonnement est en apparence parfaitement logique. Pourtant, la rationalité de l'arbitrage dépend directement de la qualité des éléments intégrés au calcul. Or plusieurs d'entre eux tendent à être sous-évalués. La probabilité d'une attaque peut tout d'abord être minorée, en particulier dans les structures qui n'ont encore jamais subi d'incident ou qui ne se considèrent pas comme des cibles particulièrement attractives. L'absence d'expérience passée devient alors, implicitement, un indicateur de faible exposition future : « cela ne nous est jamais arrivé » finit par signifier « cela a peu de chances de nous arriver ».

Surtout, les conséquences potentielles sont souvent envisagées de manière partielle. Le risque cyber reste volontiers appréhendé comme un problème technique ponctuel : restaurer un serveur, changer des postes, faire intervenir un prestataire ou remettre un service en fonctionnement. Or un incident peut produire des effets beaucoup plus diffus : interruption ou ralentissement de l'activité, désorganisation des équipes, indisponibilité de données, mobilisation de ressources internes, relations dégradées avec les clients et partenaires, coûts juridiques ou réputationnels, voire remise en cause de la continuité de l'activité. **Le coût de l'incident est alors moins celui de sa réparation technique que celui de l'ensemble des perturbations qu'il provoque.**

Cette difficulté d'évaluation est renforcée par une asymétrie très concrète : **le coût de la prévention est immédiat, visible et certain ; le coût de l'incident est futur, incertain et difficile à représenter.** D'un côté figurent un budget à débloquer, du temps à consacrer à la formation, des procédures à modifier ou des contraintes supplémentaires à accepter. De l'autre, un événement dont on ignore s'il se produira, quand il se produira et quelle en sera l'ampleur. L'arbitrage tend naturellement à favoriser ce qui est tangible dans le présent.

Dans cette représentation, les mesures fondamentales — sauvegardes testées, authentification multifacteur, segmentation, procédures formalisées, préparation à la crise — peuvent alors apparaître coûteuses au regard d'un risque perçu comme faible et réversible. **L'investissement semble disproportionné, non parce qu'il l'est nécessairement objectivement, mais parce que le périmètre du risque pris en compte dans le calcul est incomplet.**

C'est précisément là que se situe l'illusion de rationalité stratégique : le raisonnement peut être cohérent, tout en reposant sur une représentation tronquée de ce qu'il cherche à arbitrer.

Les chiffres à l'appui

- Parmi les TPE-PME qui ne se considèrent pas préparées à une cyberattaque, 61 % invoquent des contraintes budgétaires.⁹
- Et près de **30 % considèrent encore le sujet comme non prioritaire.**⁹

Analyse des mécanismes en jeu

Un facteur majeur pour expliquer cette contradiction est la faible saillance du risque cyber. C'est un risque silencieux, invisible, sans signaux faibles évidents jusqu'à l'incident. Tant qu'il n'y a pas eu d'attaque vécue ou très proche (concurrent, partenaire, voisin), le risque reste abstrait.

Et la connaissance statistique ne suffit pas à modifier cette perception. D'autant plus que les coûts immédiats des mesures de sécurité, eux, sont bien visibles et certains, (alors que les bénéfices sont hypothétiques et différés). L'investissement est donc perçu comme une charge et non une assurance.

Ainsi ce qui est présenté comme un arbitrage rationnel (ne pas investir dans la cyber) correspond souvent à une rationalité incomplète. Tant que le risque cyber n'est pas pensé comme un risque organisationnel systémique, qui relève de la gouvernance, l'investissement dans des mesures fondamentales continuera d'apparaître excessif, alors même qu'il conditionne la continuité de l'activité.



⁹ - Source : [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr/) / OpinionWay, Baromètre national de la maturité cyber des TPE-PME, octobre 2025.

TENDANCE N°6

Les petites structures surestiment l'effort nécessaire pour agir (et ont tendance à procrastiner)

Ce que l'on constate

Dans les petites structures, la perception du risque cyber prend une forme très différente de celle que l'on observe dans les grandes organisations. Comme nous l'avons vu précédemment, ces dernières disposent généralement de davantage de ressources, de fonctions spécialisées et de procédures leur permettant de penser l'incident en termes de continuité dégradée : pertes acceptables, solutions de contournement, redémarrage progressif, gestion de crise ou maîtrise des conséquences réputationnelles. Cette organisation peut entretenir une forme d'illusion d'absorption du choc : même sévère, la crise est envisagée comme quelque chose que la structure aura les moyens de gérer.

Dans une TPE ou une petite PME, le risque est beaucoup plus directement incarné. Le dirigeant sait qu'une interruption prolongée de l'activité, l'indisponibilité de ses données, la perte de son outil de production ou l'impossibilité de facturer peuvent rapidement mettre en difficulté l'ensemble de l'entreprise. Il ne raisonne donc pas nécessairement en termes de « continuité dégradée », mais dans un registre beaucoup plus immédiat : « si cela m'arrive, est-ce que mon entreprise pourra continuer à fonctionner ? » Cette proximité avec les conséquences du risque ne conduit pourtant pas mécaniquement à davantage de préparation. Elle peut même produire l'effet inverse.

Dans ce type de petite organisation, engager une démarche de cybersécurité peut donner le sentiment d'ouvrir un chantier considérable : auditer les systèmes, revoir les accès, organiser les sauvegardes, changer certaines habitudes, former les collaborateurs, interroger les pratiques des prestataires, préparer la réaction à un incident... Pris dans son ensemble, le travail à accomplir peut sembler disproportionné au regard du temps, des compétences et des moyens disponibles.

À cela s'ajoute une caractéristique non négligeable : **la préparation repose souvent sur les mêmes personnes que celles qui assurent déjà le fonctionnement quotidien de l'entreprise.** Il n'existe pas nécessairement d'équipe dédiée à laquelle déléguer le sujet. Le temps consacré à la cybersécurité est donc immédiatement perçu comme du temps soustrait à la production, au développement commercial, aux clients ou à la gestion administrative.

Le paradoxe est alors assez fort : **plus les conséquences potentielles de l'incident paraissent importantes, plus la préparation peut sembler lourde à engager.** L'ampleur perçue de la tâche peut conduire à différer le premier pas, dans l'attente d'avoir davantage de temps, de moyens ou de compétences.

La procrastination ne traduit donc pas nécessairement une absence de conscience du risque. Elle peut au contraire naître de l'écart entre l'importance accordée au problème et le sentiment de disposer des ressources nécessaires pour le résoudre. Plus cet écart paraît important, plus le passage à l'action devient difficile.

Les chiffres à l'appui

→ 87 % des TPE-PME interrogées redoutent une interruption d'activité en cas de cyberattaque.¹⁰

MAIS

→ Parmi les TPE-PME qui ne se considèrent pas préparées à une cyberattaque, 59 % invoquent le manque de temps et 63 % le manque de connaissances ou d'expertise.¹⁰

→ Seules 32 % des TPE-PME déclarent utiliser l'authentification multifacteur.¹¹

→ **15 points : c'est l'écart constaté entre la confiance déclarée des organisations et la mise en œuvre effective des mesures de cybersécurité recommandées.**¹²

Analyse des mécanismes en jeu

L'angoisse suscitée par la matérialité immédiate du risque peut paradoxalement conduire à une forme de sidération. Lorsque l'hypothèse d'un arrêt d'activité équivaut à la disparition de l'entreprise, le dirigeant est tenté de fuir cette réalité en se concentrant exclusivement sur l'opérationnel quotidien, perçu comme seul levier tangible de survie.

La préparation à un scénario de crise est perçue comme une charge supplémentaire, psychologiquement coûteuse, que l'on repousse faute de temps ou par crainte d'affronter explicitement la possibilité de l'échec.

Le déni et la procrastination sont deux modalités d'un même phénomène : la difficulté à transformer la conscience du risque en action préparatoire concrète.



¹⁰ -Sources : [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) / OpinionWay, Baromètre national de la maturité cyber des TPE-PME, octobre 2025 ;

¹¹ - Source France Num / Crédoc / Direction générale des Entreprises, [Baromètre France Num 2025](#)

¹² -Deloitte, *The Global Future of Cyber Survey*, 5e édition, 2026, section « The confidence paradox ». Enquête auprès de 1 058 dirigeants et responsables dans 43 pays. [Five paradoxes shaping the future of cybersecurity](#)

TENDANCE N°7

De manière générale, on privilégie en première intention les petites mesures visibles et ponctuelles plutôt que les fondamentaux continus

Ce que l'on constate

Face à une menace invisible, technique et souvent anxiogène comme la cyberattaque, les décideurs recherchent naturellement des réponses concrètes, immédiatement identifiables et relativement simples à mettre en œuvre. L'installation d'un antivirus, l'acquisition d'un pare-feu ou le déploiement d'un dispositif de filtrage des courriels constituent autant d'actions tangibles qui donnent le sentiment d'avoir commencé à traiter le problème.

Ces mesures sont évidemment nécessaires. Mais leur caractère visible et facilement identifiable peut conduire à leur accorder une place disproportionnée dans la représentation que l'entreprise se fait de sa propre sécurité. **L'installation d'un outil devient parfois, à elle seule, la preuve que le risque a été pris en charge.**

Or la cybersécurité ne repose pas uniquement sur l'accumulation de solutions techniques. Elle suppose également un travail continu, souvent moins visible et moins gratifiant : maintenir les systèmes à jour, gérer les droits d'accès, séparer les comptes administrateurs des comptes utilisateurs, appliquer le principe du moindre privilège, renforcer l'authentification, vérifier les sauvegardes, former les collaborateurs ou encore actualiser les procédures de réaction aux incidents.

Ces pratiques présentent une particularité : elles ne peuvent pas être considérées comme définitivement acquises. Une mise à jour en appelle une autre, les droits doivent évoluer avec les mouvements de personnel, les sauvegardes doivent être vérifiées et les procédures adaptées aux transformations de l'organisation. **Là où l'achat d'un équipement donne le sentiment d'une action achevée, l'hygiène numérique, elle, impose une vigilance permanente.**

Cette différence contribue à expliquer pourquoi certaines entreprises privilégient les investissements ponctuels, facilement budgétisables et valorisables, plutôt que des démarches de sécurisation inscrites dans la durée. L'entreprise peut ainsi disposer de plusieurs dispositifs de protection sans avoir véritablement défini qui les pilote, comment ils interagissent, comment leur efficacité est vérifiée ou comment ils doivent évoluer.

Il en résulte une forme de sécurité fragmentée : les mesures existent, mais elles ne constituent pas nécessairement un ensemble cohérent. La présence d'un antivirus ne garantit pas la bonne gestion des accès ; celle d'un système de sauvegarde ne signifie pas que les données pourront effectivement être restaurées ; l'existence d'un prestataire informatique ne garantit pas que les responsabilités ont été clairement réparties.

Les chiffres à l'appui

→ 84 % des TPE-PME interrogées déclarent disposer d'un antivirus, 78 % de sauvegardes et 69 % d'un pare-feu.¹³

MAIS

→ Seulement 24 % des TPE-PME déclarent disposer d'une procédure de réaction aux cyberattaques.¹³

Analyse des mécanismes en jeu

Le phénomène mis en évidence peut être rapproché d'un biais d'action. Les recherches en psychologie sociale montrent que l'incertitude prolongée est difficilement tolérée : l'individu cherche à rétablir une forme de contrôle, même symbolique. **L'action devient alors un instrument de régulation émotionnelle avant d'être un levier d'efficacité réelle.**

Cette dynamique apparaît avec netteté dans un contexte de stress : décider dans l'urgence, communiquer abondamment, enchaîner les réunions ou annoncer des plans correctifs relèvent parfois moins d'une réponse proportionnée que de la volonté de démontrer que « quelque chose est engagé ».

Dans la pratique, ce biais produit des effets ambivalents. Il peut favoriser une mobilisation rapide et éviter l'inertie, mais il comporte surtout un risque significatif : celui de substituer le mouvement à la réflexion stratégique. L'accumulation d'initiatives sans diagnostic stabilisé, la multiplication de chantiers parallèles ou la modification de processus sans coordination suffisante peuvent désorganiser davantage l'organisation et accentuer les difficultés initiales. L'illusion créée est potentiellement dangereuse.



¹³ - Cybermalveillance.gouv.fr / OpinionWay, 2e Baromètre national de la maturité cyber des TPE-PME, octobre 2025.

TENDANCE N°8

La technicité du risque cyber occulte sa dimension de gouvernance

Ce que l'on constate

La cybersécurité occupe une place croissante dans les préoccupations des entreprises, mais elle reste encore fréquemment traitée comme une composante de l'informatique plutôt que comme un risque transversal pour l'organisation. Dans les petites structures, elle est souvent intégrée à la relation avec le prestataire informatique ; dans les organisations plus importantes, elle relève de la DSI, du RSSI ou d'équipes spécialisées.

Cette organisation permet de mobiliser les compétences indispensables à la protection des systèmes mais elle montre ses limites dès lors que l'on considère les conséquences potentielles d'un incident. Une cyberattaque ne concerne pas seulement le fonctionnement du système d'information : elle peut interrompre la production ou la facturation, empêcher l'accès aux données, perturber les relations avec les clients et fournisseurs, engager la responsabilité de l'entreprise ou nécessiter des arbitrages financiers et réputationnels importants.

En situation de crise, cette dimension apparaît avec beaucoup plus de netteté. La question n'est rapidement plus seulement de savoir comment restaurer un serveur ou sécuriser un accès, mais quelles activités doivent être maintenues en priorité, combien de temps l'organisation peut fonctionner en mode dégradé, quelles dépenses engager dans l'urgence, quels partenaires informer ou encore à quel moment interrompre une activité.

Ces décisions ne peuvent être prises par les seuls experts techniques. Elles supposent une connaissance des priorités de l'organisation, de ses dépendances, de ses contraintes économiques et de son niveau de risque acceptable. La cybersécurité relève donc autant de la continuité d'activité et de la décision stratégique que de la protection du système d'information.

Le constat est finalement celui d'un décalage : **les manifestations du risque sont largement techniques, mais ses conséquences et les arbitrages qu'il impose sont profondément organisationnels.**

Les chiffres à l'appui

- ➔ Parmi les TPE-PME qui ne se considèrent pas préparées à une cyberattaque, 63 % des dirigeants invoquent le manque de connaissances ou d'expertise.¹⁴
- ➔ **53 % des salariés interrogés dans une autre étude internationale considèrent que la cybersécurité relève principalement des équipes informatiques ou des spécialistes de la sécurité.**¹⁵

¹⁴ - Source : Cybermalveillance.gouv.fr / OpinionWay, Baromètre national de la maturité cyber des TPE-PME, octobre 2025 ; France Num / Crédoc, Baromètre 2025.

¹⁵ - Source : KnowBe4, The State of Human Risk 2025, enquête internationale. L'étude a été réalisée par Arlington Research auprès de 3 500 salariés dans plusieurs pays, dont la France. Les répondants n'avaient pas de responsabilité directe en matière de cybersécurité.

Analyse des mécanismes en jeu

La technicité du risque cyber produit d'abord un effet de cadrage. Parce que l'incident se manifeste dans le système d'information et mobilise un vocabulaire spécialisé — vulnérabilités, pare-feu, EDR, authentification, chiffrement, architecture réseau — il est spontanément catégorisé comme un problème informatique. Or cette catégorisation détermine en partie son attribution : si le problème est technique, sa prise en charge revient logiquement au technicien, au DSI, au RSSI ou au prestataire.

Cette délégation est nécessaire pour traiter les dimensions techniques du risque. Elle devient problématique lorsqu'elle s'étend implicitement à des arbitrages qui relèvent de la direction. L'asymétrie d'expertise renforce ce phénomène : face à un domaine dont il maîtrise mal le vocabulaire et les solutions, le décideur peut considérer qu'il ne dispose pas de la compétence nécessaire pour intervenir.

Cette délégation est d'autant plus naturelle qu'elle est confortable. Face à un sujet complexe, évolutif et difficile à appréhender, confier le problème à celui qui « sait » permet également de réduire l'incertitude à laquelle le décideur est confronté. La distance technique peut ainsi progressivement devenir une distance décisionnelle.

Un glissement s'opère alors entre deux responsabilités pourtant différentes : savoir comment protéger le système et décider ce qui doit être protégé, à quel niveau et avec quels moyens. Le premier registre relève de l'expertise ; le second de l'arbitrage. Identifier les activités critiques, déterminer une durée d'interruption acceptable, fixer les priorités de reprise ou arbitrer les investissements ne nécessite pas de savoir configurer un pare-feu : cela nécessite de connaître l'entreprise et d'assumer une décision.

La technicité agit comme un écran : elle rend extrêmement visible la question du « comment se protéger », tout en pouvant reléguer au second plan les questions qui devraient la précéder : que voulons-nous protéger, contre quoi, jusqu'à quel niveau, à quel coût et qui en assume la décision ?



TENDANCE N°9

Chez les TPE/PME, il existe une dépendance forte à des prestataires externes (infogérant, agences web, éditeurs de logiciels métiers)

Ce que l'on constate

Pour de nombreuses entreprises, et particulièrement les plus petites, le recours à un prestataire informatique constitue la principale réponse aux enjeux de sécurité numérique. Faute de compétences disponibles en interne, l'externalisation est souvent indispensable. Mais la mission confiée au prestataire reste parfois insuffisamment définie : les exigences en matière de cybersécurité, les responsabilités respectives, les modalités de sauvegarde, les délais d'intervention ou encore les conditions de reprise après incident ne sont pas toujours précisément formalisés.

Cette situation entretient une confusion entre disposer d'un prestataire informatique et disposer d'une véritable capacité de protection face au risque cyber. Or les deux ne se recouvrent pas nécessairement. Un prestataire chargé de maintenir le parc informatique, d'installer les logiciels ou d'assurer l'assistance quotidienne n'est pas nécessairement spécialisé en cybersécurité, et sa mission ne comprend pas automatiquement la prévention, la détection ou la gestion d'un incident.

La même confusion apparaît autour des sauvegardes. Leur existence est fréquemment considérée comme la garantie que l'entreprise pourra reprendre son activité après une attaque. Pourtant, une sauvegarde ne constitue une véritable capacité de reprise que si l'on sait précisément ce qui est sauvegardé, à quelle fréquence, dans quelles conditions et, surtout, si sa restauration a été testée. « Avoir des sauvegardes » et « être capable de redémarrer » sont deux réalités différentes.

Deux raccourcis sont ainsi particulièrement révélateurs : considérer que « j'ai un prestataire » signifie « je suis protégé », et que « j'ai des sauvegardes » signifie « je peux redémarrer ». Dans les deux cas, **le problème n'est donc pas l'externalisation elle-même, mais l'écart entre ce que l'entreprise pense avoir confié ou sécurisé et ce qui est effectivement prévu, vérifié et garanti.**

Les chiffres à l'appui

- ➔ 36 % des TPE-PME interrogées déclarent externaliser totalement ou partiellement la gestion de leur sécurité informatique.¹⁶
- ➔ 39 % se tournent vers leur prestataire informatique pour s'informer ou obtenir de l'aide en matière de cybersécurité.¹⁶

¹⁶ - Cybermalveillance.gouv.fr / OpinionWay, 2e Baromètre national de la maturité cyber des TPE-PME, octobre 2025, questions 10 et 24, pp. 15 et 29.

Analyse des mécanismes en jeu

Deux mécanismes peuvent contribuer à expliquer cette tendance à considérer le recours à un prestataire comme une réponse suffisante au risque cyber.

1. Externaliser permet aussi d'externaliser le problème (biais de délégation)

L'externalisation peut d'abord participer à un mécanisme de réduction de la dissonance cognitive. L'entreprise sait que la menace existe et peut avoir conscience, au moins confusément, qu'elle n'est pas suffisamment préparée pour y faire face. Cette situation crée une tension entre la perception du risque et la réalité des mesures mises en œuvre.

Confier le sujet à un prestataire permet en partie de réduire cette tension : le problème est désormais pris en charge par quelqu'un dont c'est le métier. La délégation opérationnelle peut alors progressivement devenir, dans les représentations, une forme de transfert de responsabilité : « quelqu'un s'en occupe », donc « ce n'est plus vraiment de mon ressort ». Elle permet également de se décharger d'une partie de la charge mentale associée à un risque complexe, incertain et difficile à maîtriser.

La forte technicité associée à la cybersécurité renforce ce mécanisme. Parce que le sujet paraît nécessiter des compétences très spécialisées, il devient facile de considérer qu'il appartient naturellement à ceux qui « savent ». Le « je n'y comprends rien » peut ainsi conduire au « je laisse faire celui qui sait ». Or l'expertise peut être déléguée ; la responsabilité de déterminer le niveau de risque acceptable pour l'entreprise et les moyens à lui consacrer reste une question de gouvernance.

2. On a affaire à une perception parfois erronée de ce qui a réellement été externalisé

Un second mécanisme tient à la méconnaissance du périmètre réel de la prestation achetée. Le recours à un prestataire informatique peut créer le sentiment que le risque cyber est désormais pris en charge dans son ensemble, alors que la mission confiée ne couvre parfois qu'une partie des besoins de l'entreprise.

Cette confusion tient notamment à la difficulté à distinguer des prestations qui, pour un non-spécialiste, peuvent sembler relever d'un même ensemble : maintenance informatique, infogérance, sauvegarde, sécurisation des accès, supervision, détection des attaques, réponse à incident ou reprise d'activité. Or ces prestations répondent à des fonctions différentes et ne sont pas nécessairement incluses dans un même contrat. L'entreprise peut ainsi surestimer le niveau de protection associé à la prestation qu'elle achète. Avoir un prestataire informatique peut être interprété comme « être protégé contre les cyberattaques » ; disposer d'un système de sauvegarde comme « pouvoir redémarrer après une attaque ». Dans les deux cas, la prestation existe bien, mais la protection qui lui est attribuée dans les représentations dépasse son périmètre réel. La technicité du sujet renforce ce phénomène. Lorsqu'il est difficile d'évaluer soi-même la nature et la portée d'une prestation, il devient également difficile d'identifier ce qu'elle ne couvre pas. Le risque réside alors moins dans l'externalisation elle-même que dans l'écart entre la protection que l'entreprise pense avoir déléguée et celle qui a effectivement été organisée.



TENDANCE N°10

Facteur humain : on se considère rarement comme étant le maillon faible

Ce que l'on constate

À l'échelle individuelle, un paradoxe apparaît : le facteur humain est largement identifié comme une source importante de vulnérabilité, mais peu de personnes semblent se considérer elles-mêmes comme particulièrement exposées à l'erreur. Le « maillon sensible » existe, mais il est situé ailleurs.

Les collaborateurs ont généralement le sentiment d'adopter des comportements suffisamment prudents : savoir reconnaître un courriel suspect, ne pas ouvrir une pièce jointe douteuse, choisir un mot de passe adapté ou repérer une sollicitation inhabituelle. Le risque d'erreur tend alors à être associé à d'autres profils, supposés moins formés, moins vigilants ou moins familiers des usages numériques.

Il existe ainsi un décalage entre la perception du risque humain à l'échelle collective et l'évaluation de sa propre vulnérabilité. Chacun peut reconnaître que n'importe quel collaborateur est susceptible d'être trompé sans réellement intégrer qu'il appartient lui-même à ce « n'importe qui ».

Les chiffres à l'appui

- ➔ 94 % des salariés interrogés déclarent être capables de reconnaître un courriel de phishing.¹⁷

POURTANT

- ➔ 46 % reconnaissent cliquer sur des liens sans vérifier leur provenance et seuls 36 % considèrent que leurs propres pratiques numériques représentent un risque important pour leur entreprise.¹⁷

Analyse des mécanismes en jeu

1. Le collectif peut favoriser une dilution de la responsabilité individuelle

En matière de cybersécurité, chacun sait que ses comportements peuvent avoir des conséquences sur la sécurité de l'organisation. Pourtant, lorsque cette responsabilité est présentée comme collective, elle peut paradoxalement perdre de sa portée individuelle. Chacun reconnaît l'importance de la vigilance de tous, sans nécessairement mesurer le poids de sa propre contribution.

¹⁷ - Source : OpinionWay pour LockSelf, [Observatoire LockSelf 2025](#) – Les salariés de bureau et les usages numériques en entreprise, février 2025. Enquête réalisée auprès de **1 299 salariés de bureau disposant d'un ordinateur**, issus d'un échantillon de 2 111 salariés français.

Ce phénomène, connu en psychologie sociale sous le nom de dilution de la responsabilité, désigne la tendance à se sentir moins personnellement tenu d'agir lorsque d'autres personnes partagent cette responsabilité. Il peut conduire chaque collaborateur à considérer que sa vigilance individuelle ne représente qu'une contribution parmi beaucoup d'autres, et donc à sous-estimer son propre rôle dans la prévention des incidents.

À cela s'ajoute un biais d'optimisme comparatif : nous avons tendance à considérer que les événements négatifs sont davantage susceptibles d'arriver aux autres qu'à nous-mêmes. On peut ainsi reconnaître que le phishing fonctionne, que des collaborateurs peuvent être manipulés ou commettre des erreurs, tout en se considérant personnellement comme moins susceptible de tomber dans le piège.

2. La répétition des comportements à risque tend à les banaliser (biais de normalisation)

Un second mécanisme d'importance tient à la normalisation progressive des écarts. Réutiliser un mot de passe, transférer un document par un canal non prévu, contourner une procédure jugée trop contraignante ou valider rapidement une demande inhabituelle peuvent devenir des pratiques routinières dès lors qu'elles sont répétées sans conséquence apparente.

Chaque occurrence sans incident vient alors implicitement conforter l'idée que le comportement n'est finalement pas si dangereux. **L'absence de conséquence visible est interprétée comme une confirmation de l'innocuité de la pratique**, alors qu'elle signifie seulement que le risque ne s'est pas encore matérialisé.

La répétition transforme ainsi progressivement l'exception en norme : ce qui pouvait initialement être identifié comme une prise de risque finit par devenir une manière ordinaire de travailler. Et plus le comportement est partagé par d'autres membres de l'organisation, plus cette normalisation est renforcée : si « tout le monde le fait » et qu'aucun incident ne survient, le sentiment de vulnérabilité individuelle diminue encore.



TENDANCE N°11

La montée en puissance du shadow IT

Ce que l'on constate

Le shadow IT désigne l'ensemble des outils, logiciels, applications ou services numériques utilisés au sein d'une organisation sans validation ni supervision de la direction des systèmes d'information (DSI) ou du service informatique.

Il ne s'agit pas nécessairement d'actes malveillants. Le phénomène naît souvent d'un décalage entre les besoins opérationnels et les solutions officiellement mises à disposition.

Un collaborateur adopte un outil de stockage en ligne pour partager rapidement des fichiers, installe une application de gestion de projet plus ergonomique que celle imposée par l'entreprise, ou utilise une messagerie externe pour gagner en fluidité. L'objectif est l'efficacité immédiate, non la transgression.

Les conséquences peuvent être significatives en matière de cybersécurité et de gouvernance des données. Les services informatiques ignorent l'existence de ces outils ; ils ne peuvent donc ni en assurer la sécurisation ni en contrôler les accès. Des données sensibles peuvent être stockées hors du périmètre sécurisé, des comptes peuvent rester actifs après le départ d'un salarié, ou des failles de sécurité peuvent passer inaperçues. En cas d'incident, le shadow IT complique fortement l'investigation et la reprise d'activité.

Les chiffres à l'appui

- ➔ 75 % des salariés français utilisant l'IA dans leur travail déclarent recourir à des outils qui ne sont pas fournis par leur entreprise.¹⁸
- ➔ 44 % des salariés français se forment seuls à l'intelligence artificielle.¹⁸
- ➔ Seulement 15 % des salariés disposent d'une formation à l'IA et 9 % ont accès à un outil mis à disposition par leur entreprise, selon les données reprises dans le rapport sénatorial.¹⁸
- ➔ 61 % des salariés français ont déjà utilisé une adresse électronique personnelle ou un service de transfert de fichiers, comme WeTransfer, pour partager des documents professionnels.¹⁹
- ➔ 58 % des TPE-PME interrogées déclarent utiliser des équipements personnels à des fins professionnelles, contre 53 % en 2024.¹⁹

¹⁸ - Source : Sénat, [L'entreprise 5.0 : l'impact de l'intelligence artificielle sur les entreprises, rapport d'information n° 572](#), session 2025-2026, citant l'étude Saegus / Odoxa de septembre 2025. L'enquête a été réalisée du 25 avril au 2 mai 2025 auprès de 1 001 salariés utilisant l'IA dans leur travail, ainsi que d'un échantillon distinct de 1 005 adultes français

¹⁹ - Source : Cybermalveillance.gouv.fr / OpinionWay, *2e Baromètre national de la maturité cyber des TPE-PME*, octobre 2025, question 8, base : 588 entreprises.

Analyse des mécanismes en jeu

Le shadow IT témoigne d'une tension entre contrôle du système d'information et autonomie opérationnelle. Son développement est aujourd'hui facilité par la démocratisation des outils numériques, notamment en mode SaaS : quelques clics suffisent désormais pour créer un compte, transférer un document, stocker des données ou accéder à un nouveau service, sans intervention de la DSI.

D'un point de vue managérial, comprendre ces pratiques suppose de se placer du point de vue de l'utilisateur. Dans la plupart des cas, celui-ci ne cherche pas consciemment à contourner une règle de sécurité : il cherche à répondre à un besoin concret, plus rapidement ou plus simplement. Le recours à un outil externe signale un besoin insuffisamment satisfait : outil officiel jugé inadapté ou trop contraignant, fonctionnalité manquante, processus de validation trop long ou nécessité de travailler dans l'urgence.

L'utilisateur arbitre alors entre efficacité immédiate et risque potentiel. Envoyer un document sur une messagerie personnelle, utiliser un service de transfert de fichiers ou déposer des informations dans un outil d'intelligence artificielle produit un bénéfice immédiat et tangible. À l'inverse, le risque associé — fuite de données, compromission d'un compte, conservation d'informations par un tiers — reste hypothétique, différé et souvent difficile à matérialiser. Dans cet arbitrage, le bénéfice immédiat peut facilement l'emporter sur un risque dont les conséquences ne sont ni certaines ni directement visibles.

Cette logique est renforcée par une perception parfois imparfaite du risque. Un collaborateur peut connaître les principales règles de cybersécurité sans nécessairement considérer comme dangereux le fait de transférer un fichier vers son adresse personnelle ou de le déposer sur un service en ligne. La frontière entre usage pratique et comportement à risque n'est pas toujours clairement identifiée. Elle dépend également de l'évaluation que chacun fait de la sensibilité des informations manipulées : « ce document n'est pas vraiment confidentiel », « je ne l'envoie qu'à moi-même », « je supprimerai le fichier ensuite ».

À cela s'ajoute un phénomène de normalisation. Lorsqu'un outil ou une pratique est couramment utilisé par les collègues sans conséquence visible, la perception du risque tend à diminuer. Le comportement s'installe progressivement dans les habitudes de travail, d'autant plus facilement que les outils numériques grand public sont familiers, accessibles et donnent à l'utilisateur un sentiment de maîtrise (biais de normalisation).

Le contexte organisationnel peut renforcer ces mécanismes : la pression du temps, des outils jugés peu adaptés aux usages ou des procédures de validation perçues comme trop longues favorisent la recherche de solutions alternatives. **Le shadow IT ne traduit donc pas nécessairement un rejet des règles de sécurité. Il révèle plutôt un décalage entre la manière dont le risque est pensé et encadré par l'organisation et la manière dont l'utilisateur arbitre concrètement, au quotidien, entre sécurité, simplicité et efficacité.**



TENDANCE N°12

La maturité cyber est intrinsèquement liée à l'écosystème de l'organisation

Ce que l'on constate

Il existe de véritables disparités en matière de maturité cyber entre les secteurs d'activité. Dans les environnements fortement régulés ou insérés dans des chaînes de sous-traitance structurées (santé, industrie, entreprises travaillant avec de grands donneurs d'ordre, environnements de défense ou portuaires), la cybersécurité est généralement davantage formalisée. Les exigences d'audit, les clauses contractuelles, les référentiels imposés et les contrôles réguliers créent un cadre incitatif puissant. La démarche cyber y devient visible et documentée. Elle s'inscrit progressivement dans les critères de performance de l'organisation.

À l'inverse, dans certains secteurs d'activité moins soumis à ces contraintes, la nécessité de sécuriser les systèmes d'information peut rester largement ignorée, voire marginalisée. La confiance interpersonnelle, les habitudes professionnelles ou l'absence d'incidents connus peuvent tenir lieu de garanties implicites : « On se connaît », « On se fait confiance », « Nous n'avons jamais eu de problème ». La cybersécurité demeure alors une préoccupation secondaire, rarement intégrée aux processus de décision et aux investissements.

L'écosystème joue ainsi un rôle déterminant dans la construction des normes collectives de cybersécurité. Lorsqu'un donneur d'ordre exige des garanties, qu'un partenaire impose des standards ou que les pratiques de sécurité deviennent un critère d'accès au marché, les organisations sont incitées à faire évoluer leur niveau de protection. À l'inverse, lorsque ces exigences sont absentes de l'environnement professionnel, le risque cyber peut rester abstrait et les investissements difficiles à justifier. **La maturité cyber est donc le produit d'une dynamique collective : elle ne dépend pas seulement des ressources, des compétences ou de la volonté d'une organisation, mais également du niveau d'exigence de l'écosystème dans lequel elle évolue.**

Les chiffres à l'appui

- ➔ 68 % des TPE-PME de l'hébergement-restauration disposent d'au moins une mesure de cybersécurité, contre 84 % tous secteurs confondus. ²⁰
- ➔ 22 % des entreprises de l'hébergement-restauration ont mis en place des actions de formation ou de sensibilisation à la cybersécurité, contre 41 % tous secteurs confondus. ²¹
- ➔ 50 % des TPE-PME de l'hébergement-restauration disposent d'une sauvegarde externe des données, contre 68 % tous secteurs confondus. ²¹

²⁰Source : Direction générale des Entreprises / Crédoc, Baromètre France Num 2025, déclinaison sectorielle "Le numérique et l'IA dans les TPE et PME de l'hébergement-restauration", France Num, avril 2026.

- 27 % des TPE-PME de l'hébergement-restauration utilisent l'authentification multifacteur, contre 32 % tous secteurs confondus. ²¹

Analyse des mécanismes en jeu

La maturité cyber relève en partie d'un phénomène d'alignement collectif. Les organisations tendent à se comparer à leurs pairs et à ajuster leur comportement en fonction de ce qu'elles perçoivent comme la norme sectorielle. Lorsque la cybersécurité devient un standard attendu, l'investissement s'accélère. Lorsqu'elle demeure marginale, l'inaction apparaît socialement tolérable compte tenu du coût. En dehors de l'effectivité de la menace, plusieurs mécanismes sont à l'œuvre :

- **L'effet de contrainte** : les obligations réglementaires ou contractuelles créent une pression directe. L'entreprise agit non seulement par conviction, mais pour maintenir l'accès au marché.
- **L'effet mimétique** : face à l'incertitude, les organisations imitent les pratiques des acteurs perçus comme légitimes ou performants. Une attaque médiatisée dans le même secteur augmente fortement la saillance du risque et modifie les priorités collectives.
- **L'effet normatif** : lorsque la cybersécurité devient un marqueur de professionnalisme ou de sérieux, elle s'intègre progressivement aux standards implicites du métier. L'absence d'action devient alors plus coûteuse symboliquement que l'investissement.





[Notre raison d'être]

« Accompagner la résilience des organisations en leur permettant d'adapter leur communication aux grandes transitions contemporaines. »

[Nos objectifs statutaires]

Objectif 1

Être un acteur économique « colibri » qui contribue aux grandes transitions contemporaines.

Objectif 2

Placer le facteur humain au cœur des projets de l'agence.

Objectif 3

Limiter l'empreinte écologique des activités de l'agence.

Notre rapport de mission 2025 est accessible sur notre site internet.

[La boîte à mots]

Agence de planning stratégique
et société à mission

Dirigeante : Emilie Tranchant
Tel : 06 63 45 02 08
emilie@laboiteamots.fr
laboiteamots.fr

