Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

11e édition du baromètre annuel du CESIN

Etat des lieux de la cybersécurité des entreprises françaises

Le Club des Experts de la Sécurité de l'Information et du Numérique dévoile les résultats de sa 11ème grande enquête OpinionWay pour le CESIN.

Paris, le 26 janvier 2026 – Le CESIN dévoile les résultats de son baromètre annuel réalisé avec OpinionWay. Cette enquête indépendante et exclusive menée auprès de ses membres, Directeurs Cybersécurité et Responsables Sécurité des Systèmes d'Information (RSSI), analyse les grandes tendances de la cybersécurité en entreprise. Les données issues de 397 répondants apportent un éclairage unique sur la réalité concrète du risque cyber en entreprise.

Le baromètre CESIN comptabilise uniquement les cyberattaques dites « significatives », ie celles ayant entraîné un impact réel sur l'activité, les données, la conformité réglementaire ou l'image de l'entreprise. Les tentatives d'attaques stoppées par les dispositifs de sécurité, ou celles n'ayant pas eu d'impact significatif ne sont pas intégrées. Sans cette distinction méthodologique essentielle, 100% des organisations sont aujourd'hui considérées comme attaquées.

Moins d'attaques réussies, mais des impacts toujours plus lourds

En 2025, 40% des entreprises interrogées déclarent avoir subi au moins une cyberattaque[1] significative. Un chiffre en baisse continue depuis plusieurs années, or cette diminution ne traduit pas un recul de la menace, mais une amélioration progressive des capacités de détection, de prévention et de réaction rapide. En revanche lorsque l'attaque est avérée, ses conséquences restent majeures. 81% des entreprises victimes indiquent un impact sur leur business, principalement sous forme de perturbations de production, de pertes d'image ou de compromission de données. Le vol de données demeure la première conséquence de ces attaques.

1 Cyberattaque - Définition donnée pour cette enquête : « La cyberattaque est le fait de subir un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information entraînant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise et/ou des efforts significatifs de défense pour contenir et traiter l'attaque. Nous ne comptons pas les tentatives d'attaques qui ont été arrêtées par les systèmes de prévention. »

Une menace cyber de plus en plus liée au contexte géopolitique

Plus d'une entreprise sur deux estime que la menace d'origine étatique est en augmentation. Dans un contexte international instable, le cyberespionnage est désormais considéré comme un risque élevé par 40% des répondants, quelle que soit la taille de l'organisation. Ces résultats confirment que la cybersécurité dépasse largement le cadre technique pour devenir un enjeu stratégique, économique et géopolitique.

Loin d'une posture idéologique, la souveraineté est devenue un enjeu de gestion du risque. Plus d'une entreprise sur deux se déclare concernée par les enjeux de souveraineté numérique et de cloud de confiance, une hausse significative par rapport à l'an dernier.

Le baromètre montre toutefois un paradoxe, puisque la souveraineté ne se résume pas à la nationalité des outils utilisés. Elle se joue avant tout dans la capacité des entreprises à maîtriser leurs dépendances, à négocier leurs contrats, à auditer leurs fournisseurs et à reprendre la main en cas d'incident.

Les principaux risques liés au cloud, identifiés par les entreprises, sont juridiques et contractuels. Les responsables cyber pointent des clauses difficilement négociables, les lois extraterritoriales, ou encore le manque de maîtrise de la chaîne de sous-traitance.

Le risque tiers, une vulnérabilité structurelle

Un tiers des entreprises estime que plus de la moitié de leurs incidents de cybersécurité sont dus à des tiers. Les cyberattaques exploitant des failles chez des fournisseurs, prestataires ou partenaires, deviennent un vecteur majeur de compromission. Face à ce constat, les entreprises renforcent leurs dispositifs ; 85% intègrent désormais des clauses de sécurité dans leurs contrats et 74% utilisent des questionnaires de sécurité. Le cyber-rating progresse également, utilisé par près de la moitié des organisations, notamment pour évaluer leurs tiers, tandis que le taux des répondants encore réservés sur le sujet diminue ce qui souligne une amélioration de la confiance globale dans ces solutions. .

Les vecteurs d'attaque dominants restent inchangés …

…Cependant ils continuent de se structurer et de se spécialiser. Le phishing, sous toutes ses formes (phishing, spear phishing, smishing), demeure le principal point d'entrée des cyberattaques significatives, cité dans 55% des incidents. Il est suivi par l'exploitation de failles de sécurité (41%) et par les attaques indirectes via des tiers (35%), confirmant le rôle central des écosystèmes et de la chaîne d'approvisionnement dans la surface d'attaque des entreprises. Les attaques par déni de service distribué (DdoS), souvent hyper-volumétriques, concernent 21% des organisations victimes. Si leur objectif premier reste la perturbation de l'activité, ces attaques s'inscrivent de plus en plus dans des stratégies hybrides, combinant diversion, pression économique et parfois actions coordonnées dans un contexte géopolitique tendu. Parmi les vecteurs émergents, l'arnaque s'appuyant sur des technologies de deepfake est encore minoritaire, elle illustre néanmoins une évolution préoccupante des attaques d'ingénierie sociale, rendues plus crédibles et plus difficiles à détecter par l'usage de l'IA. Ces résultats confirment une tendance de fond concernant la menace, qui ne repose plus sur un unique vecteur dominant, mais sur la combinaison de techniques éprouvées et d'innovations offensives ; exploitant à la fois les failles techniques, organisationnelles et humaines des entreprises.

Des défenses plus robustes, est une forte maîtrise des actifs numériques

Les entreprises progressent nettement dans la maîtrise de leurs actifs numériques. 81% d'entre elles pensent disposer d'une vision complète de leurs actifs, tandis que 92% ont identifié ou sont en cours d'identification de leurs actifs critiques. Dans les environnements cloud, la part des organisations déclarant une mauvaise visibilité sur leur inventaire recule à 31% (-7 points). Un résultat dû à l'adoption croissante de solutions de cartographie et de pilotage des surfaces d'attaque, telles que les outils EASM et CAASM. Cette évolution marque une étape clé dans la capacité des entreprises à prioriser leur protection et à renforcer leur résilience face aux incidents.

Parallèlement, les fondamentaux de la défense restent solidement ancrés. Les solutions EDR demeurent massivement déployées. Elles bénéficient d'un très haut niveau de confiance, avec 95% d'efficacité perçue, tandis que l'authentification multi-facteurs s'impose désormais comme un standard. Les approches structurantes poursuivent leur montée en puissance, 31% des entreprises déclarent avoir engagé une démarche Zero Trust (+7 points) et 26% disposent d'un Vulnerability Operation Center (+9 points), in fine c'est une cybersécurité de plus en plus pilotée dans la durée et intégrée à la gouvernance.

.. mais des fragilités persistantes

Si les entreprises progressent nettement sur la visibilité et la protection de leurs actifs, la gouvernance fine des identités et des usages demeure l'un des principaux défis à relever. Le baromètre met en évidence des points de fragilité persistants, comme la gestion des accès à privilèges, notamment ceux des administrateurs et des sous-traitants, tout comme la sécurisation d'environnements toujours plus hybrides et distribués.

L'intelligence artificielle s'impose comme un nouveau facteur de risque cyber

L'IA ouvre une nouvelle surface d'attaque. Le recours par les salariés aux services d'IA non approuvés (shadow IA) est identifié comme le comportement numérique le plus risqué, 66% des entreprises le jugent à risque élevé ou très élevé. Plus largement, 60% considèrent également l'usage massif de services cloud ou logiciels non approuvés comme un facteur de risque important, révélant une perte de contrôle croissante sur les usages numériques liés à l'IA.

Si l'exploitation directe de l'IA comme vecteur d'attaque est encore marginale, elle apparaît déjà dans des incidents significatifs, citée par 3% des entreprises victimes. Un signal faible à surveiller dans un contexte où l'IA renforce rapidement ses capacités offensives, telles que l'automatisation, celle des malwares capables d'adapter leur comportement en temps réel, ou les premiers codes malveillants autonomes réécrivant partiellement leur logique pour échapper à la détection. L'IA est donc à la fois un levier d'innovation, mais aussi un enjeu de cybersécurité à part entière, appelant des réponses structurées en matière de gouvernance, de contrôle des usages et de protection des données.

La pression réglementaire continue de s'intensifier

En 2025, 85% des entreprises déclarent être impactées par au moins une réglementation cyber, confirmant une progression nette par rapport aux années précédentes. La directive NIS2 s'impose comme le cadre le plus structurant, citée par 59% des organisations, devant DORA 32% et le Cyber Resilience Act, CRA (30%). Cette montée en puissance des exigences réglementaires renforce l'intégration durable de la conformité dans les stratégies de cybersécurité, avec des impacts directs sur la gouvernance, les processus et les choix technologiques des entreprises.

Des priorités qui se stabilisent, une gouvernance qui s'installe durablement

Cette nouvelle édition du baromètre confirme l'ancrage durable du risque cyber dans les priorités des entreprises. En 2025, 92% des organisations positionnent le risque cyber dans leur Top 5 des risques, et près de deux tiers (64%) le placent désormais dans le Top 3, dont 16% comme risque numéro un. La cybersécurité n'est plus un sujet émergent, elle est pleinement intégrée aux dispositifs de gouvernance et fait l'objet d'un suivi régulier en comité de direction.

Sur le plan budgétaire, le baromètre met en évidence un léger infléchissement. La part des entreprises consacrant 5% ou plus de leur budget IT ou numérique à la cybersécurité recule à 42%, contre 48% l'an dernier. Cette baisse ne traduit pas un désengagement, mais plutôt un changement de posture après plusieurs années d'investissements soutenus, les entreprises semblent entrer dans une phase de consolidation et d'optimisation des dispositifs existants, plutôt que dans une logique d'expansion continue.

Du côté des compétences et de la formation, les fondamentaux restent solides. La sensibilisation des collaborateurs demeure un levier central, 85% estiment que les utilisateurs sont aujourd'hui sensibilisés aux risques cyber, un niveau stable par rapport à l'an dernier. En revanche, le baromètre souligne plus clairement l'atteinte d'un « plafond de verre » en matière de sensibilisation, pointant les limites de ce levier face à des usages numériques toujours plus complexes, notamment liés au cloud et à l'IA.

Dans l'ensemble, les résultats traduisent une évolution de la maturité des organisations. La cybersécurité n'est plus abordée sous l'angle de l'urgence ou de la montée en puissance des moyens, mais comme une fonction stratégique à piloter dans la durée, arbitrée au plus haut niveau et intégrée aux choix de gouvernance globale.

« Baromètre annuel de la cybersécurité des entreprises »
« Sondage OpinionWay pour le CESIN réalisé en ligne de décembre 2025 à janvier 2026 auprès des membres du CESIN ».
Retrouvez ici l'intégralité des résultats du sondage OpinionWay pour le CESIN.

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels. Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.

Le CESIN rassemble plus de 1 200 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120. Pour en savoir plus www.cesin.fr