



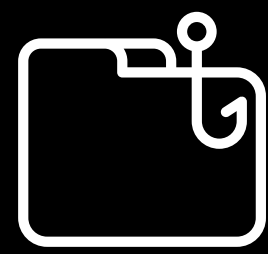
Baromètre de la cybersécurité 2025

Troisième édition

Un sentiment de maîtrise du risque en décalage avec l'exposition réelle.

Si **1/3** des organisations a subi une cyberattaque en 2025, **2/3** pensent pourtant que le risque est faible ou modéré.

Les cyberattaques les plus courantes :



38 %

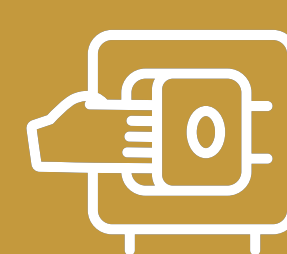
Phishing

+15 % en 2025



28 %

Ransomware



17 %

Vol/Perte de données

Et leurs conséquences :



24 %

Blocage des systèmes d'information



21 %

Vol et/ou perte de données

+40 % en 2025



13 %

Arrêt de la production

Top 3 des protections mises en place :

89 %

Gestion renforcée des mots de passe

85 %

Mise à jour régulière des logiciels

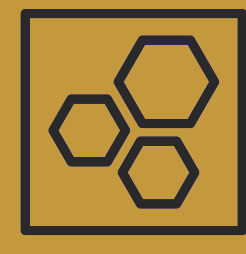
81 %

Sauvegarde externalisée et régulière des données

+55 % des budgets cybersécurité sont en hausse (notamment dans le secteur public)



3/4 des entreprises pensent faire suffisamment d'efforts pour se protéger



Près d'**1** entreprise sur **2** privilégie des solutions packagées de cybersécurité



1/3 des répondants connaît et applique le guide de l'ANSSI*

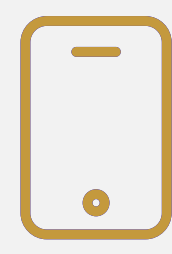
*Agence nationale de la sécurité des systèmes d'information

La souveraineté, essentielle dans le secteur public :

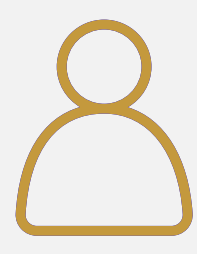
55 % des acteurs publics considèrent l'usage des systèmes souverains comme très important

vs **37 %** des entreprises privées

Méthodologie du baromètre



Sur la base d'entretiens téléphoniques



517 répondants



Part importante d'acteurs publics (**26 %**)

Le Baromètre de la cybersécurité, co-réalisé par Docaposte et Cyblex Consulting, permet de mesurer année après année l'évolution de la maturité cyber des entreprises et des organisations publiques.