

La gestion des risques de cybersécurité



**Comment évaluer
les vulnérabilités
de votre entreprise
et mettre en place
des mesures
de prévention
adaptées ?**

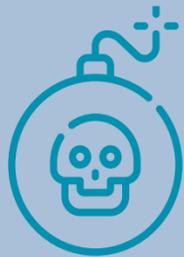
Lire la suite



Que sont les risques de cybersécurité ?

Les risques cyber sont **des menaces potentielles qui exploitent les vulnérabilités des systèmes d'informations.**

Avec **la transformation numérique des entreprises**, ils sont toujours plus nombreux. Voici les principaux types :



Logiciels malveillants

Programmes informatiques conçus pour endommager, perturber ou voler des données



Phishing

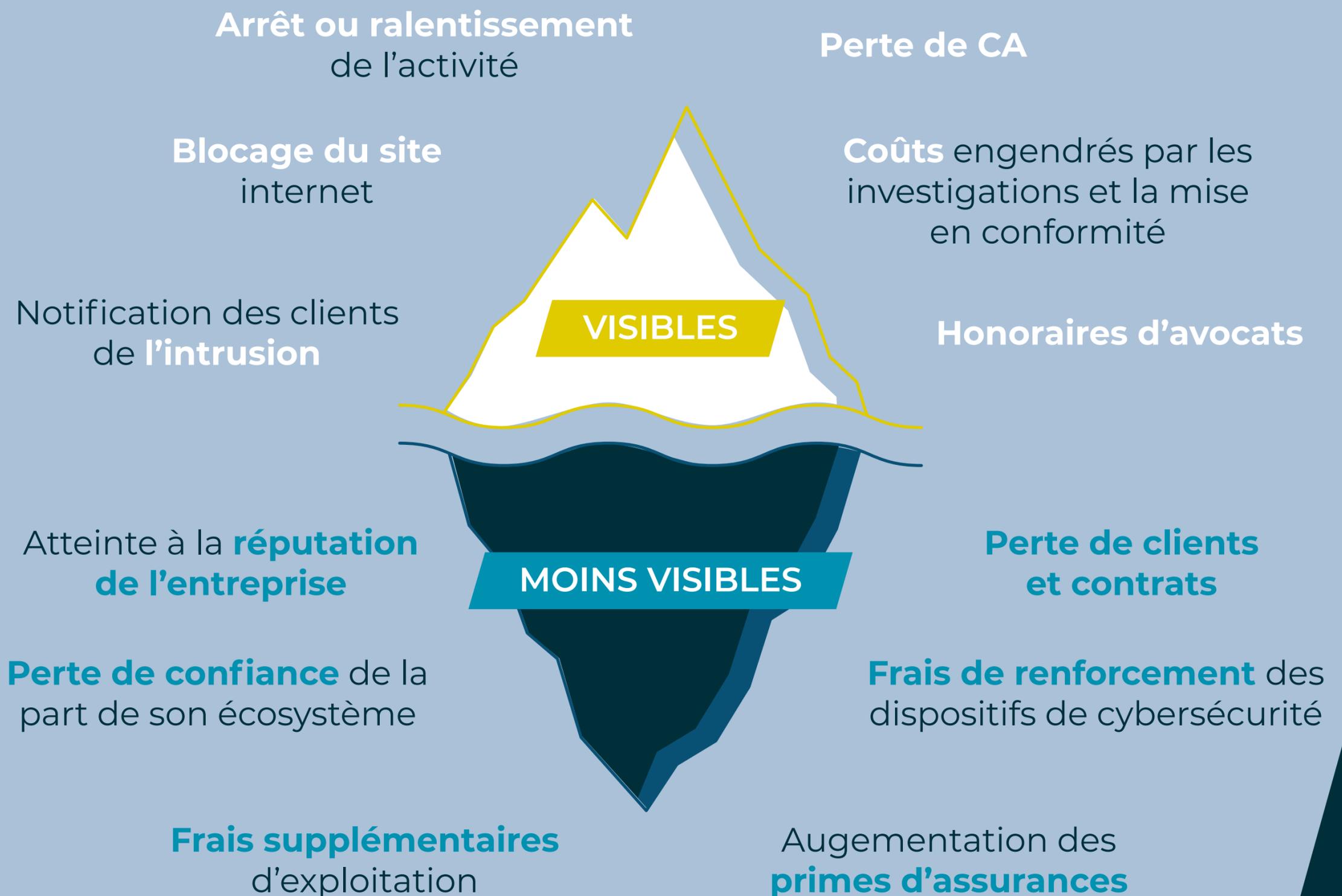
Technique de cyberattaque utilisant de faux e-mails, sites web ou messages pour soutirer des informations personnelles ou sensibles



Ransomwares

Logiciels malveillants bloquant l'accès aux fichiers ou systèmes informatiques, exigeant une rançon pour les débloquer

Quelles sont les conséquences pour les entreprises ?



Comment évaluer les vulnérabilités de votre entreprise ?

L'évaluation **des points faibles de votre système d'information** peut être réalisée à l'aide :

D'outils automatisés

- > Ils scannent **les systèmes informatiques de votre entreprise** pour identifier **les faiblesses potentielles**

D'analyses de code

- > Elles examinent **le code source des logiciels utilisés par votre entreprise** pour identifier les failles de sécurité

De tests de pénétration

- > Ils simulent **des attaques réelles sur vos systèmes informatiques** pour identifier leurs vulnérabilités

D'examens des configurations des systèmes

- > Ils analysent **les paramètres de sécurité et les configurations de vos systèmes informatiques** pour détecter les erreurs de configuration

Comment mettre en place des mesures de prévention adaptées ?

Une fois les vulnérabilités identifiées, il est essentiel **d'instaurer des mesures de protection** pour réduire les risques cyber :

Mettre en place des solutions techniques

Pares-feux, antivirus, systèmes de détection d'intrusion, outils de gestion des accès, etc.

Sensibiliser vos collaborateurs

Communication interne, formations, simulations de cyberattaques, conseils et bonnes pratiques, etc.

Définir des politiques de sécurité et des processus de gestion des incidents

Pour pouvoir réagir rapidement en cas d'attaque et maintenir la continuité de votre activité.

> Il est recommandé d'organiser **des exercices de crise**

/ Pour en savoir plus...

Vous souhaitez en savoir plus
sur ***les documents la gestion
des risques de cybersécurité ?***

Découvrez notre article sur :

 **www.implid.com**

implid