

#32

Observatoire de la CYBERSÉCURITÉ

En bref



**Près de 15 000 entreprises normandes
victimes de cyberattaques en un an**

PROTECTION

72 % des entreprises ont nommé une personne **chargée de la protection des Systèmes d'Information**

26 % des entreprises ont **augmenté leurs dépenses de sécurité informatique**

Les principales difficultés : **manque de temps, coûts et manque de compétences**

CYBERATTQUES

15 000 entreprises normandes ont été **victimes d'une ou plusieurs cyberattaques**

L'industrie, les services aux entreprises et la construction sont les secteurs les plus impactés

Les principales attaques : **Phishing, arnaques aux faux ordres de virement et logiciels malveillants**

CONSÉQUENCES

1 entreprise victime sur 5 déclare que la **poursuite de son activité a été mise en danger** et estime avoir **perdu du chiffre d'affaires**

1 entreprise victime sur 3 déclare avoir **engager des dépenses supplémentaires** pour résoudre leur cyberattaque





La cybersécurité dans les entreprises normandes

Le développement du numérique a considérablement révolutionné le quotidien des entreprises, en transformant leur façon de travailler, de communiquer et d'interagir. L'intelligence artificielle constitue désormais un accélérateur de cette profonde transformation des environnements professionnels.

Face à ces mutations, la menace reste omniprésente et en constante évolution. Les niveaux de vulnérabilité et de protection des entreprises varient en fonction de leur taille mais aussi de leur secteur d'activité. Cette deuxième édition de l'observatoire de la cybersécurité permet de dresser une nouvelle photographie de la maturité cyber des entreprises normandes et de mesurer sa prise en compte dans ces structures économiques.

LES ACTIONS DE CYBERSÉCURITÉ DÉPLOYÉES

Pour faire face à la menace omniprésente et en constante évolution, 93 % des dirigeants interrogés déclarent avoir mis en place des actions de cybersécurité dans leur entreprise. Cette part s'élève à 97 % dans les entreprises de plus de 50 salariés.

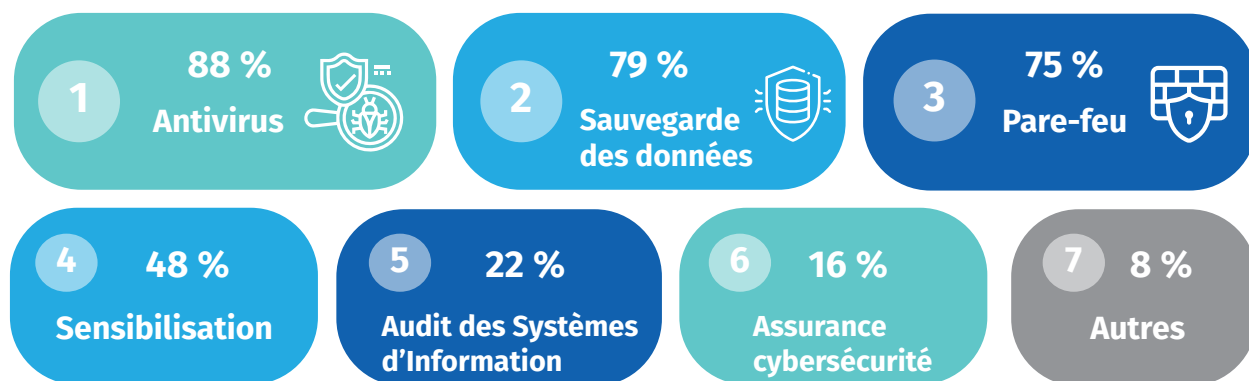
Les actions déployées sont avant tout d'ordre matériel. L'installation d'antivirus figure comme le premier dispositif de sécurité mis en place (88 %), devant les systèmes de sauvegarde des données (79 %) et l'usage de pare-feu (75 %) ①.

Dans les établissements employeurs, la sensibilisation du personnel est une action relativement déployée (63 %) tout comme l'audit du système d'information (34 %). Enfin, moins d'une entreprise sur cinq a souscrit à une assurance cyber.

Graphique ①

Quel(s) dispositif(s) de sécurité avez-vous mis en place ?

Source : Enquête « Observatoire de la cybersécurité » des CCI de Normandie



À RETENIR

26 %

des entreprises ont augmenté leurs dépenses de sécurité informatique

LES INVESTISSEMENTS RÉALISÉS

Des investissements en hausse sont observés pour réduire les risques mais des disparités budgétaires persistent en fonction de la taille des entreprises et du secteur.

Globalement, les dirigeants déclarent une stabilité des dépenses de sécurité informatique sur les 12 derniers mois. Face aux risques croissants de cyberattaques, une entreprise sur quatre a tout de

même augmenté ses dépenses en termes de protection informatique. Plus d'un établissement de plus de 50 salariés sur trois a augmenté ses dépenses.

Sur les 12 derniers mois, 3 secteurs d'activité ont davantage investi en sécurité informatique : l'industrie, les services aux entreprises et la construction.

LES DIFFICULTÉS RENCONTRÉES

Si plus d'une entreprise sur six considère ne pas affronter de difficultés dans la mise en place d'une démarche de cybersécurité, 23 % estiment manquer de temps pour la déployer.

Cette difficulté est avancée dans la majorité des entreprises, quelle que soit sa taille ou son secteur d'activité.

Le coût et le manque de compétences sont des difficultés

rencontrées par respectivement 23 % et 16 % des dirigeants.

Enfin, le manque de vision stratégique est avancé pour 4 % des chefs d'entreprise.

CHIFFRES CLÉS

72 %

des entreprises ont nommé une personne chargée de la protection des systèmes d'information

LES RESSOURCES & RGPD

72 % des entreprises ont nommé une personne chargée de la protection des systèmes d'information.

L'internalisation et l'externalisation de cette tâche ont le même poids (40 %). A noter que près de 30 % des établissements de plus de 50 salariés ont recours aux 2 modes.

Par ailleurs, il faut noter que 11 % des entreprises souhaitent assurer

leur conformité réglementaire notamment en termes de RGPD.

Ainsi une entreprise sur deux dispose d'un Délégué à la Protection des Données (DPD) en charge de piloter cette mise en conformité et cette ressource est internalisée pour 85 % d'entre-elles. 62 % des entreprises de plus de 50 salariés ont un DPD.

LES CYBERATTAQUES SUR LES 12 DERNIERS MOIS

Au cours des 12 derniers mois, c'est environ 15 000 entreprises normandes qui ont été victimes d'une ou plusieurs cyberattaques. La moitié d'entre-elles ont d'ailleurs été victimes de plusieurs cyberattaques.

Des disparités selon la taille des entreprises s'observent de nouveau.

Les plus petites entreprises, souvent dépourvues de ressources financières et d'expertise nécessaires, sont les plus impactées.

7 entreprises normandes victimes d'une cyberattaque sur 10, sont des entités comprenant moins de 50 salariés. Ce ratio reste identique à celui du premier observatoire de la cybersécurité.

Les secteurs d'activité les plus ciblés sont l'industrie, les services aux entreprises et la construction. Ce dernier ayant été particulièrement impacté sur les 12 derniers mois, avec de nombreux cas « d'arnaque au président ».

À RETENIR

15 000
entreprises
normandes victimes
d'une ou plusieurs
cyberattaques



Graphique 2

De quel(s) type(s) de cyberattaque avez-vous été victime ?

Source : Enquête « Observatoire de la cybersécurité » des CCI de Normandie

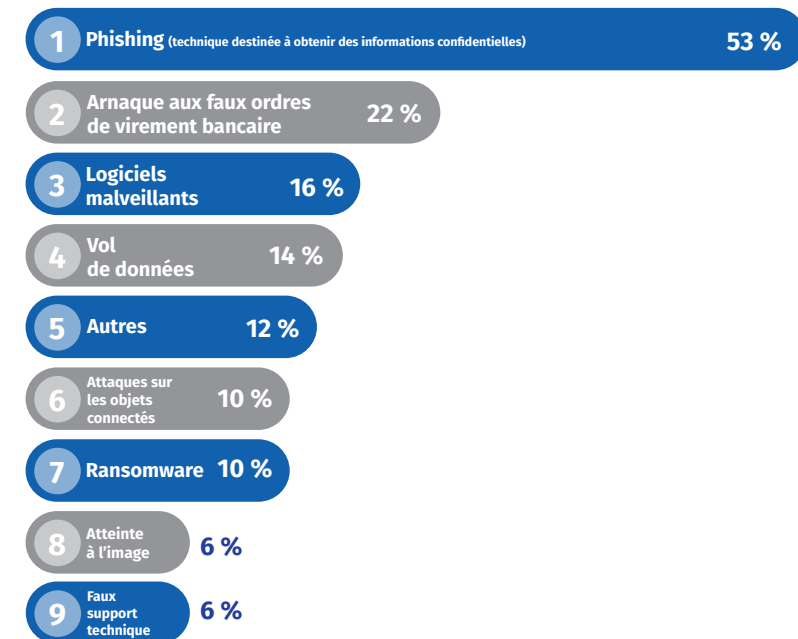
Le phishing demeure le premier vecteur d'attaque touchant plus d'une entreprise sur deux (53 %) 2. Cette technique s'élève à 75 % dans le secteur de la construction.

Si globalement, les arnaques aux faux ordres de virement bancaire impactent 22 % des entreprises, le commerce de détail et les services aux particuliers sont les principaux secteurs affectés par cette technique avec respectivement 60 % et 50 % des attaques.

L'usage de logiciels malveillants (cheval de troie, virus, ...) complète le podium.

Non seulement la typologie d'attaque varie selon le secteur d'activité, mais elle varie aussi selon la taille de l'entreprise.

Ainsi, le vol de données touche davantage les entreprises de plus de 50 salariés (27 % d'entre elles). A noter qu'en cas de violation de données personnelles, l'entreprise peut être tenue responsable juridiquement de cette perte



d'information et que des poursuites judiciaires et des amendes peuvent en découler.

L'usage et le développement des parcs d'objets connectés (smartphones, tablettes,)

augmentent la surface d'attaque au sein d'une entreprise. Les attaques ciblant ces objets connectés augmentent également en proportion et touchent 18 % des entreprises de plus de 50 salariés.



DES CONSÉQUENCES ÉCONOMIQUES

Au final, une entreprise sur cinq ayant vécu une cyberattaque, déclare que la poursuite de son activité a été mise en danger et estime avoir perdu du chiffre d'affaires ³.

Cela touche une entreprise de moins de 50 salariés sur cinq. Majoritairement, la perturbation de la production ou encore l'indisponibilité du site web ont duré plusieurs semaines.

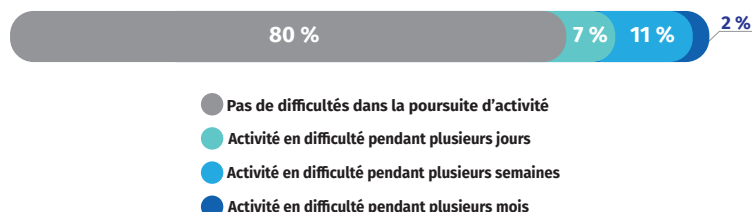
La résolution des cyberattaques peut engendrer un coût financier supplémentaire aux investissements réalisés pour se protéger.

Près d'une entreprise sur trois déclare avoir engagé des dépenses supplémentaires pour résoudre leur cyberattaque (20 % à moins de 5 000 € et 12 % à plus de 5 000 €). Cette perte financière touche principalement les petites entreprises de moins de 50 salariés.

Graphique 3

Ces cyberattaques ont-elles mis en danger la poursuite d'activité de votre entreprise ?

Source : Enquête « Observatoire de la cybersécurité » des CCI de Normandie



LES PRIORITÉS DES DIRIGEANTS

Les cybercriminels ajustent très régulièrement leurs tactiques mais s'attaquent particulièrement aux salariés, premières portes d'entrée dans les systèmes informatiques.

La sensibilisation des collaborateurs aux enjeux de cybersécurité demeure la priorité pour 47 % des dirigeants.

En effet, les campagnes de sensibilisation et d'éducation

représentent un premier rempart aux attaques.

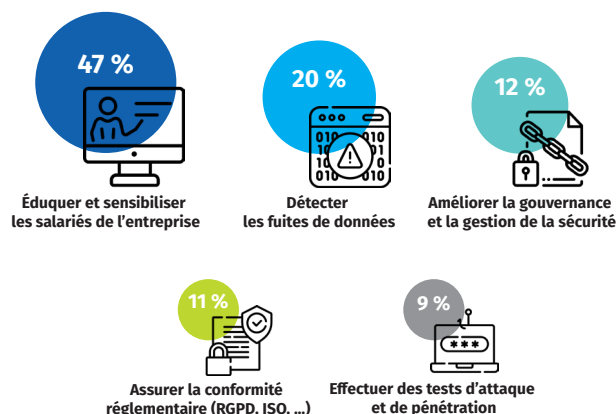
Cette part est naturellement plus élevée dans les établissements employeurs.

20 % des dirigeants considèrent la détection des fuites de données comme prioritaire et 13 % jugent qu'il est primordial d'améliorer la gouvernance et la gestion de la sécurité ⁴.

Graphique 4

Selon vous, quelle est la priorité en matière de cybersécurité ?

Source : Enquête « Observatoire de la cybersécurité » des CCI de Normandie



Observatoire de la CYBERSÉCURITÉ

#32 | Septembre 2024

CCI Observatoires

Publication économique de CCI Normandie
ISSN : 2427-5360

Directeur de la publication : Vincent Laudat

Une réalisation du Pôle Projets Innovants, Financements et Territoires

T 02 35 88 38 11
pi@normandie.cci.fr

Rédaction et mise en page : Frédéric Allais

CCI Normandie
4 passage de la luciline
76000 ROUEN

Note méthodologique :

• Recueil des données : enquête téléphonique réalisée entre le 23 mai 2024 et le 04 juin 2024 par la société Prestance

• Traitement des données : CCI Normandie

• Étude réalisée auprès d'un échantillon représentatif de 523 dirigeants d'établissement normands (degré de certitude : 95 % - marge d'erreur : +/- 4 %)

• Représentativité par secteur géographique, secteur d'activité et tranche d'effectif (moins de 5 salariés*, de 5 à 49 salariés, 50 salariés et plus)

f Normandinamik

cci-normandie

in CCINormandie

CCI NORMANDIE

normandie.cci.fr