CYBER PROTECTION

Côte-d'Or ATTRACTIVITÉ

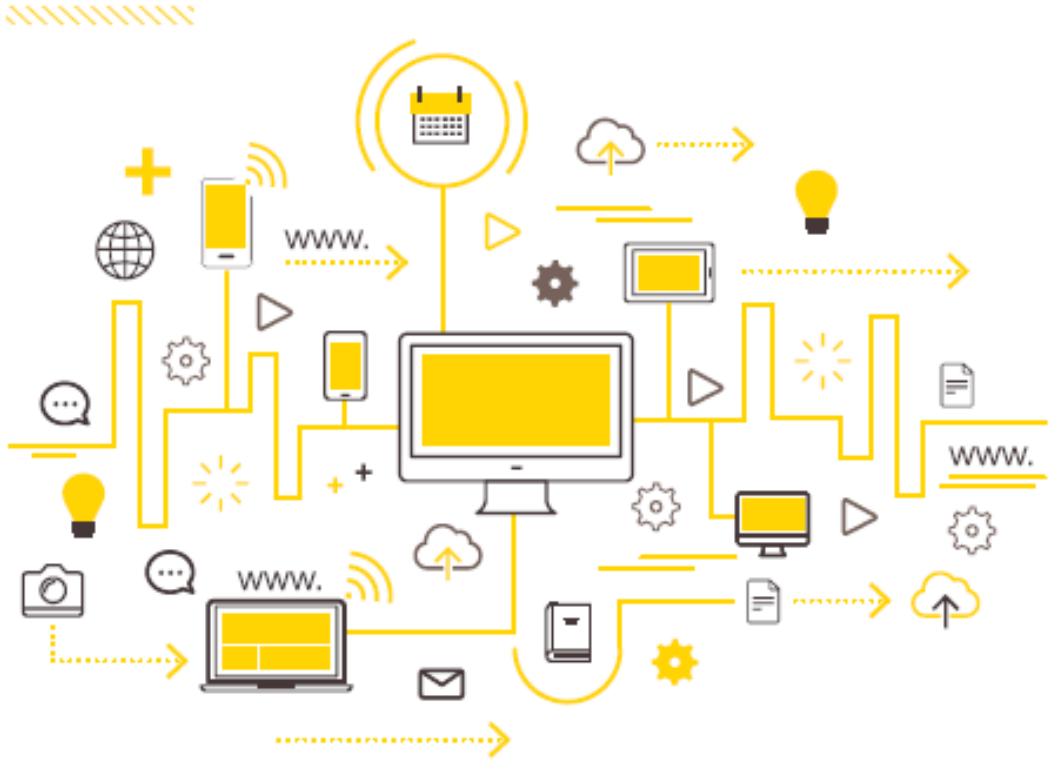
HISCOX

ASSURANCES


404
PAGE NOT FOUND

Cyber attaque = braquage virtuel

La cyber attaque : c'est une intrusion dans le système informatique par un cybercriminel pour voler des données et/ou de l'argent afin d'obtenir un gain financier



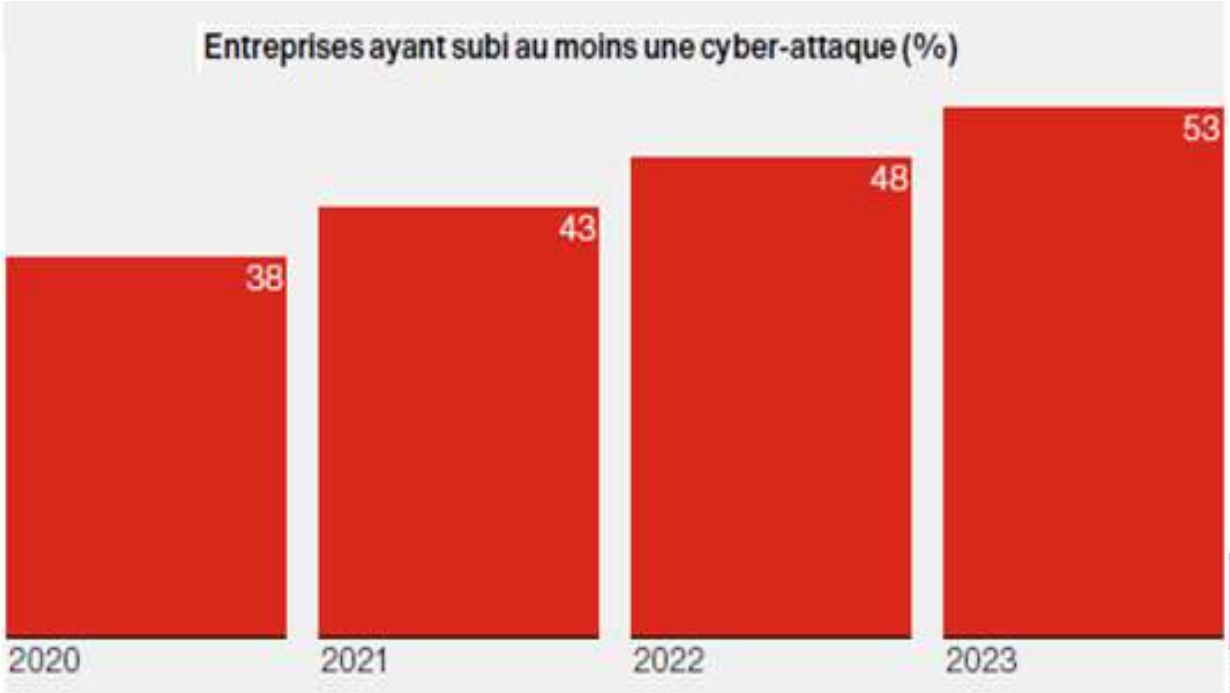
Source : Guide de la Cybersécurité pour les TPE/PME (2021) édité par BPI FRANCE

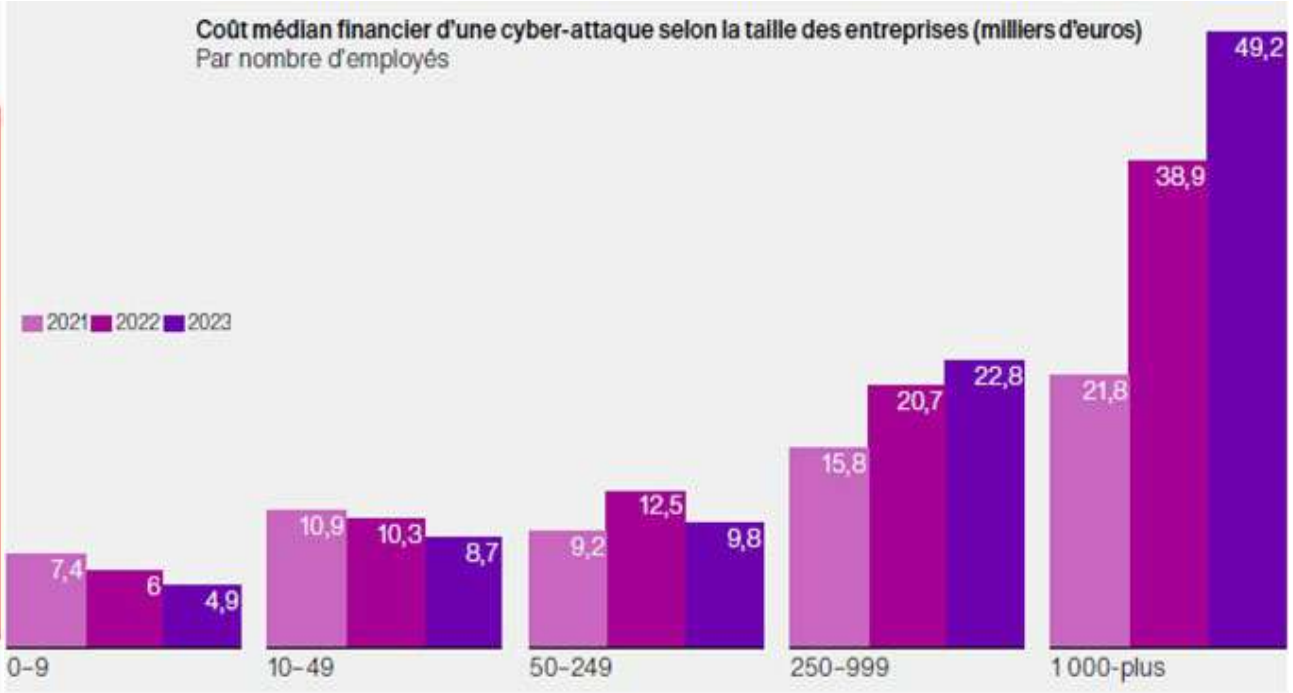
Quelques chiffres :

- La France est le 4ème pays le plus touchée au monde par les cybers attaque
- 1 entreprise sur 2 attaquée en France
- 1 entreprise touchée peut en contaminer 150 autres
- 1 entreprise sur 6 ne se relève pas d'une cyber attaque

Cyber
Définition et chiffres clés

La cyber attaque : c'est une intrusion dans le système informatique, il s'agit d'un acte malveillant qui peut émaner d'une personne seule, comme d'une organisation très structurée de cybercriminels. Les atteintes portent sur les données (vol et revente sur le dark net) et/ou sur les valeurs (fraude au virement).
Un seul objectif: obtenir un gain financier





Source: Rapport Hiscox 2023

Rançongiciel (Ransomware)

Source : infrographie_rançongiciels_ransomwares.pdf (cybermalveillance.gouv.fr)

Pourquoi ?

- Une activité rentable pour les cyber-pirates en raison du paiement des rançons pas les entreprises
- Utilisation de la cryptomonnaie : pas de traçabilité possibilité

+255 % d'attaques par ransomware

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a constaté une **hausse de 255 % des attaques par rançongiciel** (ou ransomware) contre les organisations françaises en 2020 par rapport à 2019.

ACTUALITE

HISCOX

Côte-d'Or ATTRACTIVITÉ

ASSURANCES

Piratage informatique: un vigneron escroqué de 41000 euros témoigne

Des experts en sécurité dévoilent les méthodes et les astuces des cybercriminels pour anéantir des systèmes informatiques ou rançonner des entreprises. Un vigneron victime témoigne.

Les entreprises sont souvent beaucoup plus vulnérables au piratage informatique qu'elles ne le croient. Les délinquants du numérique adaptent en permanence leurs méthodes pour tromper la vigilance des utilisateurs.

Journal « L'Union » - Reims

Franche-Comté

Des garagistes Renault victimes d'une cyberattaque d'ampleur : "On doit travailler comme dans les années 80 avec des tableaux Excel"

Sur les 3000 agents Renault, 600 seraient concernés, en France, par cette attaque informatique de pirates ayant exfiltré de nombreuses données : fichiers, historiques clients, garanties ou bilans comptables.

Véronique OLIVIER - 28 nov. 2021 à 06:30 | mis à jour le 29 nov. 2021 à 14:23 - Temps de lecture : 2 min

Vu 6467 fois

Les garagistes ont subi une cyber attaque cet été et certains doivent s'adapter en attendant une solution du groupe Solware. Photo ER /Lionel Vadam

L'Est Républicain

Les cyber attaques et leurs conséquences

***ZOOM** Phishing : Technique frauduleuse destinée à leurrer la victime pour l'inciter à communiquer ses données (ex : impôts)*

ASSURANCES

Côte-d'Or ATTRACTIVITÉ

Les 3 principales cyber attaques :

« Rançongiciel »
Blocage des données et demande de rançons

« Intrusion dans le SI »
Intrusion dans le SI pour altérer le fonctionnement ou dérober des données

« Déni de service »
Prise de contrôle par un cybercriminel du SI

Les conséquences pour l'entreprise :

Conséquences financières
Ex: perte de CA / perte financière suite transactions frauduleuses ou retard de livraison, frais de défense, indemnité, etc.

Conséquences opérationnelles
Ex: perturbations voire arrêt de la production, compromission des informations, indisponibilité du site web, etc.

Conséquences réputationnelles
Ex: mauvaise presse, mauvaise communication interne et/ou externe

Conséquences réglementaires
Ex: sanction par une autorité avec un impact négatif sur les affaires ou sur le CA

Les données sensibles utilisées par les entreprises

Toutes les données sont concernées :

Données confidentielles de l'entreprise

Eléments de propriété intellectuelle	Données stratégiques	Données d'exploitation
• Droits d'auteur • Marques • Dessins, modèles • Protection des bases de données par le droit sui generis	• Base de données clients • Données financières sur l'entreprise, ses fournisseurs et ses clients • Plan de développement • Projets de fusion ou d'acquisition	• Données techniques • Données de production

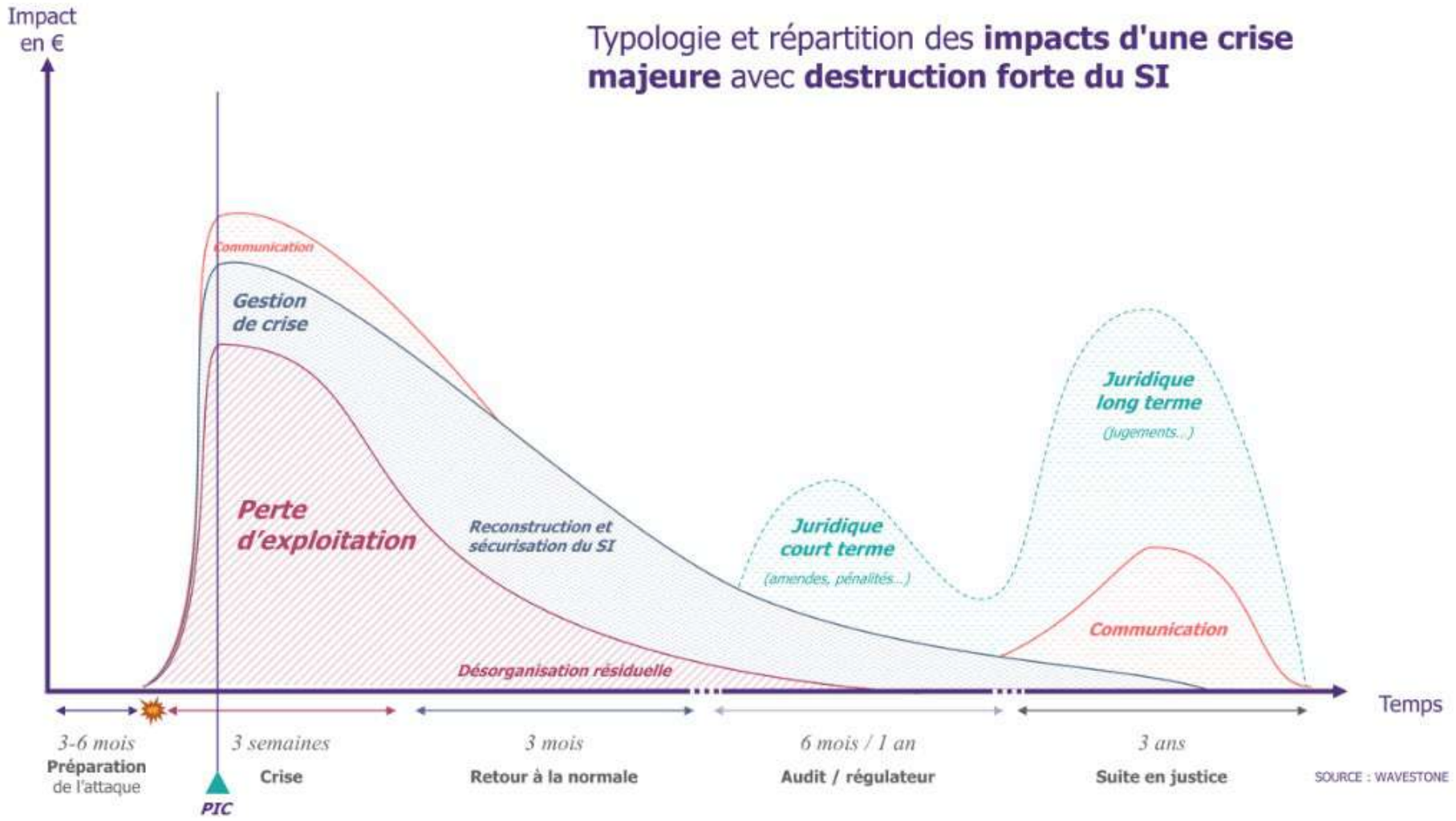
Depuis 2018, les données collectées, traitées et stockées par les entreprises sont protégées par le Règlement Général sur la Protection des Données (RGPD)

Données personnelles

Données individuelles	Données bancaires	Données médicales
Les informations relatives à des personnes physiques identifiées ou identifiables, directement ou indirectement (ex. nom, adresse, email, téléphone) : • Données des salariés • Données clients • Données fournisseurs	• Numéro de carte de crédit • RIB / IBAN • Numéro de chèque • Identifiant et mot de passe d'accès à une banque en ligne Toutes données potentiellement soumises au secret bancaire	• Antécédents médicaux • Numéro de sécurité sociale (très recherché au marché noir, car ce sont des données pérennes (non « réinitialisables »)

CNIL
+24 % de notifications pour violation de données par rapport à l'année dernière

Conséquence d'une cyber attaque



EXEMPLES DE SINISTRES REGLES

HISCOX

Côte-d'Or ATTRACTIVITÉ

CA ASSURANCES

Exemple sinistre restaurant :

- ***Type d'attaque : Ransomware***
- ***Conséquences :***
  - ***Intégralité du système d'information chiffré***
  - ***Caisses physiques affectées rendant toute transaction impossible***
- ***Aspects financiers:***
  - ***Coût de la rançon: 5 000€***
  - ***Coûts informatiques: 17 000€***
  - ***Perte d'exploitation: 23 000***

Virement frauduleux

Activité : Société de Service

Suite à une intrusion d'un pirate dans le système informatique de l'entreprise, le DAF (salarié) a reçu un faux email usurpant la véritable adresse du dirigeant avec une demande de virement de 75 000 € sur un compte bancaire désigné.
Croyant la demande authentique, le salarié a débloqué les fonds, ni la banque de la société, ni la banque destinataire n'ont réussi à recouvrer les fonds par la suite.

Prise en charge Hiscox
En réalisant ce qui s'était passé, la société a appelé l'assistance de son contrat Cyber Protection. L'expert en sécurité informatique a circonscrit l'attaque, confirmer l'intrusion et il y a eu remboursement des fonds volés.

Frais d'assistance : 3 500 €
Remboursement de la fraude : 70 000 € déduction de la franchise de 5 000 €

- Activité : Hôtel
- Type attaque : Ransomware
- Vecteur d'intrusion : Accès distant (ouvert pour que le prestataire ait accès au SI) exploité par l'attaquant
- Conséquences :
  - Données chiffrées : base client, messagerie inutilisable
  - Impossible d'utiliser l'application métier, hotel fermé pendant 2 jours
- Aspect financier :
  - Réponse à incident : 4,5ke
  - Investigations numériques : 7ke
  - Accompagnement CNIL + Com : 4ke
  - Perte d'exploitation : 18ke

JEUX-LES-BARD, commune de 52 Habitants escroquée de 9000 Euros après le piratage de la boîte mail

En 2023, les investissements dans la petite commune de Jeux-lès-Bard, dans le canton de Semur-en-Auxois, risquent fortement d'être au ralenti. En effet, la municipalité de ce village de 52 habitants a été victime d'une escroquerie au faux ordre de virement. Il s'agit d'une arnaque d'un nouveau genre qui se répand en France. Les mairies sont autant ciblées que les professionnels et les particuliers. À Jeux-lès-Bard, les faits remontent à fin septembre 2022. Des personnes mal intentionnées ont réussi à se faire payer par la mairie une facture de 9 000 € en lieu et place d'un entrepreneur local, la SARL Thomas Garrot. Cette entreprise, basée à Forléans et spécialisée dans les travaux de plâtrerie et de peinture, était chargée de la rénovation de la salle du conseil municipal.

Conséquences indirectes de l'augmentation des cyber attaques

Investisseurs et repreneurs tiennent compte des risques cyber dans l'évaluation des entreprises qu'ils convoitent. Une société mal préparée peut perdre jusqu'à 20 % de sa valeur. Alors avant d'ouvrir son capital ou de vendre, un audit informatique complet s'impose.

https://business.lesechos.fr/entrepreneurs/numerique-cybersecurite/0700759774258-risque-cyber-perte-de-valeur-de-20-environ-pour-une-entreprise-mal-preparee-347553.php

UNE BONNE OFFRE CYBER

L'assurance Cyber Protection

Communications et dédommagements des clients et fournisseurs dont les données ont été utilisées à leur insu

Accompagnement en cas de demande de Ransomware (demande de rançon)

Indemnisation du client pour la récupération des données perdues par l'entreprise, remise en place du système d'informations, prise en charge des frais de notifications éventuels ou réparation de la cyber fraude

En option : couverture de la perte d'exploitation liée à la perte de données ou au blocage du système d'information

Un réseau d'experts reconnu proposant des prestations « sur mesure », 24h/24 et 7jrs/7 sans franchise

On **A**ssiste

- expert sécurité informatique
- expert restauration données
- avocat obligations légales
- expert gestion de crise

On **R**épare

- réparation du système d'informations
- réparation des données
- frais de notification aux clients
- dommages-intérêts

On **P**aye

- interruption d'activité (option)
- cyber-fraude et surfacturation téléphonique
- rançon, en dernier ressort

17

Les critères d’éligibilité

Qui peut souscrire ?

- Tous statuts juridiques
- Toutes entreprises dont le chiffre d’affaires est inférieur à 50 millions d’€ HT par an

Quelques rares exclusions…

- Portails et processeurs de paiement
- Activités contraires aux bonnes mœurs
- Activités opérant sur les crypto-monnaies
- Les compagnies aériennes
- Nucléaire, aéronautique, aérospatial
- Jeux d’argent
- Les institutions financières et assurances
- Fournitures d’utilité (eau, gaz, électricité)
- Hébergement de données

Le Cyber Calculateur Hiscox

HISCOX

Côte-d'Or ATTRACTIVITÉ

ASSURANCES

1. Renseignez votre profil

Responsable d'une petite entreprise
Je suis responsable des décisions de l'entreprise. Mes connaissances en matière de cybersécurité sont limitées, je veux en savoir davantage.

Gestionnaire des risques
C'est mon travail de connaître la cybersécurité et les risques associés.

Courtier
J'agis pour le compte de mes clients afin de leur trouver la couverture adaptée.

Haut dirigeant
Je suis responsable principal de la gestion des cyber-risques dans une organisation de moyenne ou grande taille.

Je ne sais pas si mon entreprise est une cible d'attaques sophistiquées, mais je sais que la menace est réelle et qu'elle pourrait engendrer de graves perturbations. Par où commencer ?

2. Renseignez les caractéristiques de votre entreprise

Choisissez les caractéristiques qui décrivent le mieux votre organisation.

Secteur d'activités	Région	Revenus (en devise locale)
Commerce et vente au détail	UE	Jusqu'à 1 M

L'estimation financière de votre exposition aux cyber-risques

€143.8 K

Qu'est-ce que l'exposition aux cyber-risques ?

Il s'agit d'une estimation de la perte financière maximale (« pire scénario ») qu'une organisation comme la vôtre (c'est-à-dire du même secteur d'activités, située dans la même région et générant des revenus semblables) pourrait subir l'année suivante en cas de cyber-incident, avec un degré de fiabilité élevé (95 %). Cependant, il s'agit uniquement d'une estimation; la perte financière pourrait être plus ou moins élevée selon la nature exacte de votre activité et les circonstances particulières de l'attaque.

Ventilation de votre exposition aux cyber-risques

Nous avons défini quatre catégories de pertes distinctes qui couvrent les principales formes possibles de cyber incidents.

Type de cyber-risques

Interruption d'activités
Coûts induits du fait de l'indisponibilité des systèmes de gestion des activités et/ou des systèmes informatiques (par ex. attaque par ransomware chiffrant l'ensemble des systèmes informatiques)

Informations à caractère personnel
Coûts induits du fait de l'exposition des informations qui peuvent identifier une personne ou qui sont liées à une personne (par ex. le nom, les informations sur sa santé/son emploi, les informations financières, etc.)

Actifs immatériels
Coûts induits par le vol des ressources qui représentent une valeur pour une organisation et qui ne sont pas matérielles par nature (par ex. les licences, droits d'auteur, brevets, marques, etc.)

Perte financière
Coûts directs ou indirects résultant d'une fraude financière, de réclamations, d'amendes, d'exigences supplémentaires de reporting, etc.

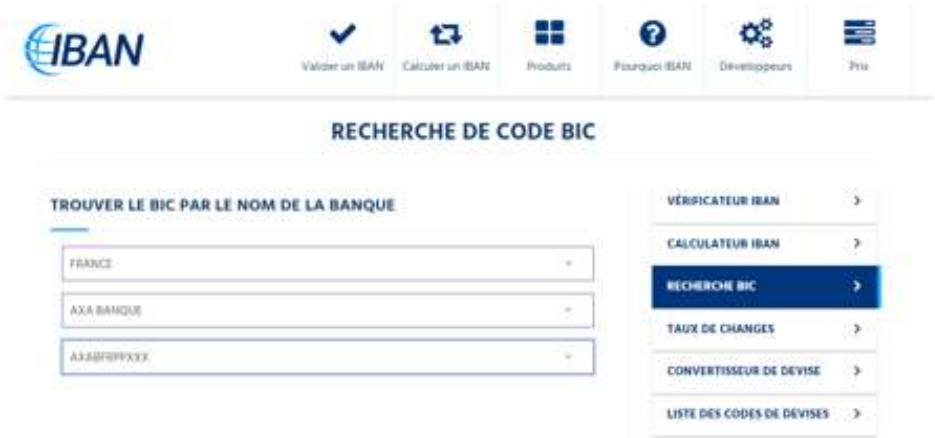
Veuillez noter que certains de ces coûts peuvent ne pas être assurables

https://www.hiscox.fr/calculateur-exposition-cyber-risques/

Trucs & Astuces

Un site de vérification pour checker si les adresses email n'ont pas été compromises : **https://haveibeenpwned.com /** utile pour voir si des pirates peuvent potentiellement avoir accès à votre boite mail.

Un site pour vérifier le code BIC du RIB : **https://fr.iban.com/recherche-bic (iban.com)** utile pour contrôler les RIB transmis et éviter les virements frauduleux à des fournisseurs en identifiant : nom de la banque, pays de la banque, ville de la banque et adresse de la banque émettrice



Que faire en cas de cyber attaque ?

HISCOX

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Côte-d'Or ATTRACTIVITÉ

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

QUE FAIRE EN CAS DE CYBERATTAQUE ? (dirigeants)

Méthodologie synthétique de gestion des cyberattaques pour les dirigeants des entreprises, associations, collectivités, administrations.

1 PREMIERS RÉFLEXES

Alertez immédiatement votre support informatique si vous en disposez afin qu'il prenne en compte l'incident (service informatique, prestataire, personne en charge).

Isolez les systèmes attaqués afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.

Constituez une équipe de gestion de crise afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique...).

Tenez un registre des évènements et actions réalisées pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.

Préservez les preuves de l'attaque : messages reçus, machines touchées, journaux de connexions...

NE PAYEZ PAS DE RANÇON !

Car vous encourageriez les cybercriminels à chercher à vous attaquer à nouveau et financeriez leur activité criminelle tout en n'ayant aucune garantie qu'ils tiendront leur parole.

2 PILOTER LA CRISE

Mettez en place des solutions de secours pour pouvoir continuer d'assurer les services indispensables. Activez vos plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.

Déclarez le sinistre auprès de votre assureur qui peut vous dédommager voire vous apporter une assistance en fonction de votre niveau de couverture assurantielle.

Alertez votre banque au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.

Déposez plainte avant toute action de remédiation en fournissant toutes les preuves en votre possession.

Identifiez l'origine de l'attaque et son étendue afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.

Notifiez l'incident à la CNIL dans les 72h si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels.

Gérez votre communication afin d'informer avec le juste niveau de transparence vos administrés, clients, collaborateurs, partenaires, fournisseurs, médias...

FAITES-VOUS ACCOMPAGNER

Par des prestataires spécialisés en cybersécurité que vous pourrez trouver sur **www.cybermalveillance.gouv.fr.**

Que faire en cas de cyber attaque ?

3 SORTIR DE LA CRISE

Faites une remise en service progressive et contrôlée après vous être assuré que le système attaqué a été corrigé de ses vulnérabilités et en en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.

Tirez les enseignements de l'attaque et définissez les plans d'action et d'investissements techniques, organisationnels, contractuels, financiers, humains à réaliser pour pouvoir éviter ou a minima pouvoir mieux gérer la prochaine crise.

PRENEZ EN COMPTE LES RISQUES PSYCHOLOGIQUES

Une cyberattaque peut engendrer une surcharge exceptionnelle d'activité et un sentiment de sidération, d'humiliation, d'incompétence voire de culpabilité susceptible d'entacher l'efficacité de vos équipes durant la crise et même au-delà.

CONTACTS UTILES

Conseils et assistance

Dispositif national de prévention et d'assistance aux victimes de cybermalveillance
www.cybermalveillance.gouv.fr

Notification de violation de données personnelles

Commission nationale informatique et liberté (CNIL)
www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Police – gendarmerie : 17

Autres sites à connaître

HISCOX

Côte-d'Or ATTRACTIVITÉ

ASSURANCES

ANSSI | Agence nationale de la sécurité des systèmes d'information

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

www.cnil.fr

LA SÉCURITÉ DES DONNÉES PERSONNELLES

Gendarmerie

WWW.GENDARMERIE.INTERIEUR.GOUV.FR

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE