ANTICIPER ET MINIMISER L'IMPACT D'UN CYBER RISQUE

Entreprises, commerçants, artisans, collectivités territoriales, **vous êtes tous concernés**

Fédération Française de l'Assurance

Avant-propos

Se protéger des risques cyber n'est plus une option pour les acteurs économiques d'aujourd'hui, c'est un enjeu vital. Quelle que soit leur taille, les entreprises doivent préserver leur savoir-faire, leurs compétences et leurs données sensibles face à des attaques malveillantes aux conséquences potentiellement dévastatrices.

Le métier de votre assureur est la gestion des risques. À ce titre, il est votre partenaire privilégié pour vous accompagner dans la maîtrise de ces nouveaux défis. En effet, se prémunir des risques cyber, c'est garantir au mieux votre résilience et votre compétitivité.

Vous trouverez dans ce guide les bonnes pratiques à adopter pour anticiper et minimiser l'impact d'un risque cyber et poursuivre ainsi le développement de votre entreprise avec sérénité.

Florence LUSTMAN
Présidente de la Fédération
Française de l'Assurance

SOMMAIRE

CYBER-RISQUES

Cela leur est arrivé...

- **En surfant sur le net, un architecte a vu apparaître une fenêtre de sécurité l'informant de la contamination de son ordinateur par un virus et bloquant toutes fonctionnalités.** Des messages se sont affichés l'invitant à contacter un support technique qui, avant toute intervention, lui a réclamé le paiement d'une facture de 500€. L'architecte a réglé la facture mais aucune intervention n'a été réalisée le laissant avec un ordinateur hors service.

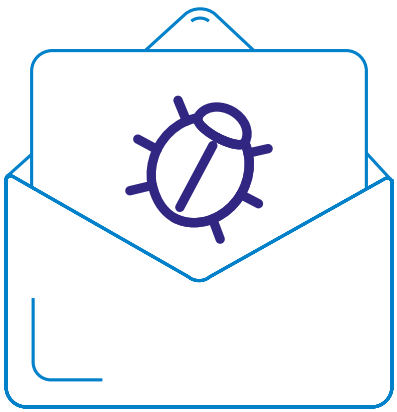
- Bien qu'il bénéficiât d'un contrat de prestations informatiques prévoyant anti-virus et sauvegardes hebdomadaires, **un cabinet d'expertise-comptable a définitivement perdu les bilans de ses clients à la suite d'une attaque cyber.** Aucune mise à jour de l'antivirus, ni test de sauvegarde n'avaient été réalisés par le prestataire informatique depuis plus de 6 mois.

- **En pleine saison estivale, une station balnéaire du Var est attaquée.** Les serveurs informatiques de la municipalité sont infectés, les fichiers sont cryptés et une rançon est exigée. Les services des ressources humaines et de la comptabilité ainsi que l'office de tourisme sont hors service pendant plusieurs jours.

- **Un collaborateur d'une entreprise sous-traitante de la filière automobile s'est connecté au réseau Wi-Fi non-sécurisé de l'hôtel** dans lequel il résidait. Après une journée de négociation avec son plus important client, il transmet à son DG par mail des données confidentielles (prix unitaire, volume commandé, délai de fabrication). Une semaine plus tard l'entreprise apprend que son principal concurrent a emporté le marché sur la base d'une offre identique à la sienne, mais à un prix inférieur et un délai de livraison plus court.

- **En mai 2019 une grande ville des États-unis a été victime d'une cyber attaque.** Afin d'éviter la propagation du virus, plusieurs milliers d'ordinateurs de son réseau ont été mis hors ligne. Pendant un mois, le courrier électronique de la ville et le système de vidéo-surveillance de la ville n'ont pas fonctionné. Les services de gestion de l'eau et de l'immobilier ainsi que la délivrance des permis de conduire ont été très fortement perturbés.

Avez-vous anticipé la survenance de tels incidents sur votre organisation ?



En quoi suis-je concerné par les cyber-risques ?

- Tout ou partie de mon activité dépend-elle d'un outil informatique (mail, système d'information, objets connectés…) ?

- Des données permettant l'identification de tiers (clients, collaborateurs…) sont-elles stockées et / ou traitées par mon entreprise ?

- En cas d'incident informatique (cyber attaque, erreur humaine), mon entreprise serait-elle affectée, à plus ou moins long terme, si je ne pouvais plus accéder à mon système d'information ou à mes données ?
  - Une baisse significative de mon chiffre d'affaires pouvant aller jusqu'à la liquidation judiciaire de mon entreprise peut-elle être envisagée ?
  - Suis-je en risque vis-à-vis de la réglementation ?
  - Suis-je susceptible d'être mis en cause par mon donneur d'ordre ? par mes salariés ? par des tiers ?

- Association sans but lucratif, collectivités territoriales la fuite de données personnelles concernant mes membres ou mes concitoyens peut-elle remettre en cause le fonctionnement de mon organisation ?

Que vous ayez ou non des réponses satisfaisantes à ces questions,
vous devez être conscients des cyber risques et vous en protéger…

Une maîtrise absolue de la sécurité des systèmes d'information n'est jamais acquise !

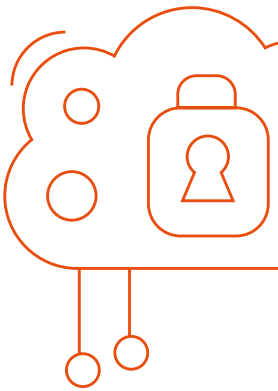
Un **transfert du risque à votre assureur** est nécessaire au cas où un cyber attaquant parviendrait à contourner vos protections.

Protéger mon organisation

La sûreté informatique de votre organisation passe d'abord par une démarche d'analyse de votre exposition à ces nouveaux risques, puis par la mise en place d'une politique de prévention adaptée avant de transférer le risque à votre assureur.

Cette analyse doit être individuelle et spécifique à votre organisation.

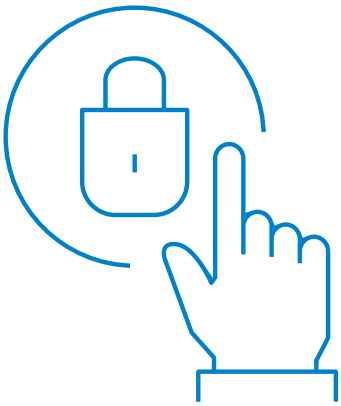
Elle doit être portée par un responsable, clairement identifié en charge de la mise en place et du suivi de cette politique de management du risque cyber.



Cette politique doit reposer sur 4 piliers :

- **les facteurs humains et organisationnels,**
- **des outils de protection,**
- **des outils de résilience,**
- **une anticipation de la gestion de crise.**

Retrouvez en page suivante les bonnes pratiques et outils à mettre en œuvre pour réduire votre risque cyber et faciliter son assurance.



▶ FACTEURS HUMAINS

1. La lutte contre les cybers risques commence par une sensibilisation / formation de l'ensemble des collaborateurs de l'entreprise à la vigilance et aux bonnes pratiques.

En vol : vous n'ouvrez pas la porte à n'importe qui.

En Cyber : n'ouvrez pas vos systèmes d'information à n'importe qui !

2. Au-delà de vos collaborateurs, vos sous-traitants et prestataires doivent également être sensibilisés et formés contre ces risques. Ils ne doivent pas représenter le maillon faible de votre protection face aux cyber menaces.

Dans certains cas, ces mesures, notamment de formation, relèvent d'une obligation légale (art 39 du Règlement général sur la protection des données (UE) 2016/679)

▶ FACTEURS ORGANISATIONNELS

1. La gestion des droits d'accès et des mots de passe

La gestion des droits d'accès, tant physiques qu'informatiques, doit être adaptée à la situation de votre organisation et aux fonctions des collaborateurs concernés. Une véritable politique de gestion des droits doit être mise en place au sein de votre organisation.

Pour éviter qu'ils soient facilement usurpés, vos mots de passe doivent être individualisés, secrets, robustes (complexes) et régulièrement changés.

C'est le nombre de caractères dont il est constitué et non les caractères spéciaux qu'il contient qui rend un mot de passe robuste.

Un mot de passe avec 16 caractères simples est plus robuste qu'un mot de passe avec 8 caractères spéciaux.

2. Le respect de règles simples d'hygiène informatique

La totalité du personnel intervenant dans l'organisation, collaborateurs, chef d'entreprise, dirigeants, CDD, stagiaires, alternants compris, doit respecter quelques règles pour lutter au quotidien contre les cyber risques.

Des règles simples doivent être rappelées régulièrement :

- Éviter l'utilisation des appareils personnels (clefs USB ou disques durs externes) ainsi que les accès distants ou mobiles non sécurisés (wifi, bluetooth).
- Ne pas laisser en évidence ses mots de passe sur son bureau et utiliser un gestionnaire de mots de passe,
- Verrouiller son ordinateur à chaque fois que vous quittez votre poste de travail,
- Élaborer des règles de consultation des mails et pièces jointes douteux (liens hypertextes, extensions .pif, .com, .exe, .bat, .lnk).

Ces règles doivent également être partagées avec l'ensemble de vos partenaires, fournisseurs, prestataires.

3. La mise à jour régulière de tous vos logiciels (de comptabilité, de production, de gestion, etc)

Les failles de vos logiciels sont autant de chemins d'accès pour des intrusions malveillantes. N'attendez pas qu'une faille soit à l'origine d'un incident cyber pour remplacer ou mettre à jour le logiciel concerné. Il est impératif de suivre et appliquer régulièrement les patchs ou correctifs communiqués par les éditeurs de logiciels.

▶ OUTILS DE PROTECTION

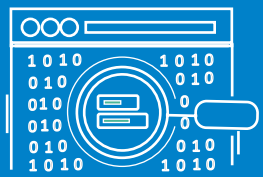
La protection de votre organisation passe par la mise en place d'outils adaptés à la valeur de vos données ainsi qu'à votre dépendance à votre système d'information. Après une analyse centrée sur **vos spécificités,** vous pouvez, notamment, mettre en place :

ANTI-VIRUS ET PAREFEUX

Sont la base de la protection indispensable de tous systèmes d'information. Ils doivent être mis à jour de manière régulière, au mieux quotidiennement, et de manière automatique.

OUTILS DE FILTRAGE

Le parefeux est efficacement complété par des outils de surveillance de type « Intrusion Protection System » (IPS) qui filtrent les entrées et les sorties pour détecter et écarter un certain nombre d'intrusions malveillantes.



OUTILS ET SERVICES DE SURVEILLANCE ET DE DÉTECTION

1/ Surveillance opérée par IDS* (Intrusion Detection System) corrélée avec un SIEM* (Security Information and Event Management).

2/ Scanners de vulnérabilités*, outils d'identification de vulnérabilités des systèmes d'informations (SI).

3/ SOC* (Security Operations Center), plateforme de supervision et d'administration de la sécurité des systèmes d'informations.

* Voir rubriques « Questions fréquentes »

▶ OUTILS DE RÉSILIENCE

La capacité de l'organisation à redémarrer rapidement après une attaque s'anticipe, notamment, sur les trois axes suivants :

1. LES SAUVEGARDES

- Organiser une sauvegarde fréquente de vos données, idéalement quotidienne, sur des supports et systèmes distincts de votre système d'information. Tester, au moins annuellement, les restaurations pour vérifier qu'elles sont exploitables.
- Eviter de localiser vos sauvegardes sur le même site que celui hébergeant déjà les systèmes et données à sécuriser.

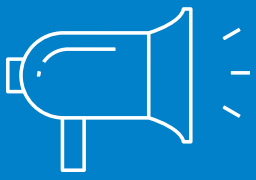
Les sauvegardes de vos systèmes d'exploitation et progiciels doivent suivre les prescriptions des sites éditeurs et celles de vos prestataires informatiques.

2. LE PLAN DE CONTINUITÉ D'ACTIVITÉ

Il comprend un Plan de Reprise d'Activité, dédié au redémarrage du système d'information, qui vous prescrit de :

- Détecter et évaluer les risques liés à vos données (personnelles et confidentielles), systèmes d'exploitation et applications afin de définir vos besoins en termes de sauvegardes et de restauration.

- Mettre en place une procédure de gestion de crise en cas de survenance d'une attaque.
- Nommer des collaborateurs (managers, experts, communicants) mobilisables sans délai, en charge d'appliquer les mesures d'urgence nécessaires pour assurer la continuité ou à défaut une reprise la plus rapide possible de l'activité de votre organisation.



3. L'ANTICIPATION DE LA GESTION DE CRISE

Votre organisation doit mettre en œuvre des processus afin de gérer au mieux la crise. A titre d'exemples, voici des services pouvant être proposés par votre assureur :

- Une ligne téléphonique d'urgence, disponible 24h/24 et 7J/7 ;
- L'accès à des consultants et experts (informatiques, juridiques, en organisation, communication et gestion de crise) ;
- L'analyse d'impacts de la situation et élaboration d'un plan d'actions de remédiation de l'incident ;
- La recherche de cause (Forensic).

Assurer mon organisation

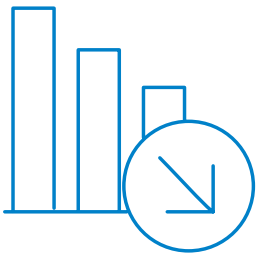
Le risque cyber impacte toutes les dimensions de votre organisation : vos biens, vos responsabilités, votre exposition médiatique.

Pour protéger et assurer ce qui m'appartient : mon patrimoine et mes actifs

▶ Deux solutions complémentaires :

▸ **Les contrats de dommages aux biens** couvrent notamment les incendies dont ceux qui ont pour origine une attaque cyber.

Exemple : attaque virale sur le boitier de commande d'une machine-outil numérique qui entraine un échauffement de cette dernière puis un incendie



▸ **Les contrats cyber, en complément, peuvent couvrir :**

• Les frais de reconstitution de données*.

• Les pertes d'exploitation consécutives à l'atteinte à vos données, à la sécurité ou à la disponibilité du système informatique.

• Les principaux frais résultants d'une fuite de données personnelles et/ou confidentielles qui vous appartiennent ou vous sont confiées.

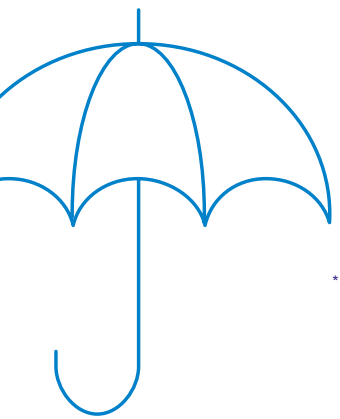
Exemples : les frais de déclaration d'incident (ou frais de notification) au régulateur, les frais d'information aux personnes concernées et les frais induits par l'enquête administrative.

Pour assurer ma responsabilité vis-à-vis des tiers :

- **Les contrats de responsabilité civile générale** couvrent la réparation financière de dommages matériels, corporels et/ou immatériels causés à des tiers (clients, voisins, salariés…) lorsque ma responsabilité est engagée. Ces contrats peuvent couvrir également les frais de retrait et les frais de dépose-repose des produits livrés ou travaux réalisés susceptibles d'entrainer des dommages et d'engager votre responsabilité.

- Pour les dommages matériels, immatériels et/ou corporels causés aux tiers du fait d'une attaque informatique dont votre organisation est victime, la couverture de ces dommages peut être comprise ou non dans votre **contrat d'assurance responsabilité civile générale.**

  Il est important de vérifier ce point avec votre assureur.



* La reconstitution des données doit être réalisée à partir de documents et de sauvegardes informatiques disponibles et exploitables

Pour vous accompagner en cas de crise :

A la suite d'un incident cyber, les contrats cyber vous accompagnent dans la gestion de la crise et ainsi en limiter l'impact tant financier, qu'en terme d'image. Votre assureur peut prendre en charge :

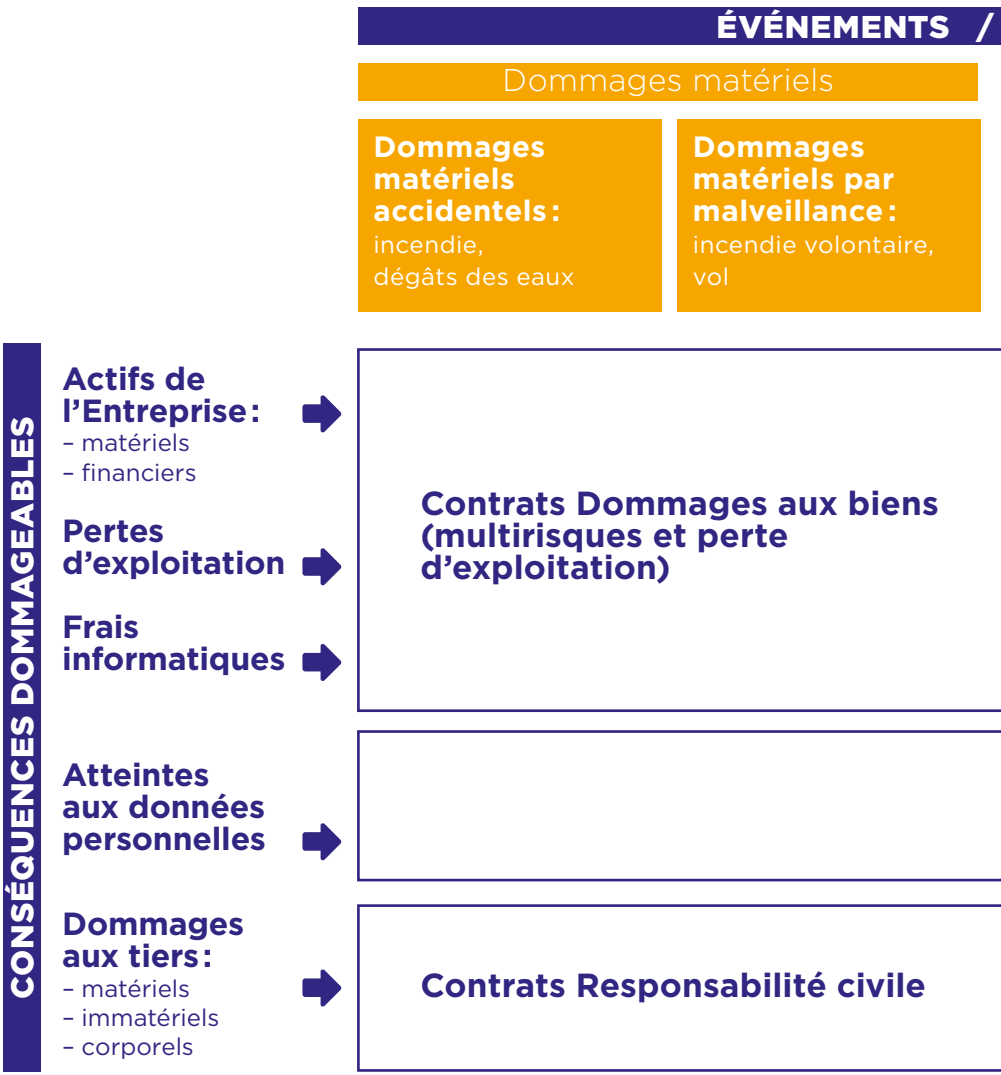
- La mise à disposition d'une plateforme de gestion de crise ;
- Des frais de consultants spécialisés en vue de faire cesser une cyber-extorsion ;
- Des frais de gestion de crise, comme des frais de communication et/ou de préservation de la réputation et de l'image de votre organisation.
- Les frais de décontamination du système, frais d'expertise en sécurité informatique.
- Les frais de consultants juridiques, les frais de défense juridique.
- Dans certains cas (souvent en option) les pertes financières directes résultant d'une fraude informatique.

Il est important de se rapprocher de son assureur conseil afin de bien identifier l'intervention, l'articulation et la nature des garanties délivrés par ces différents types de contrats.

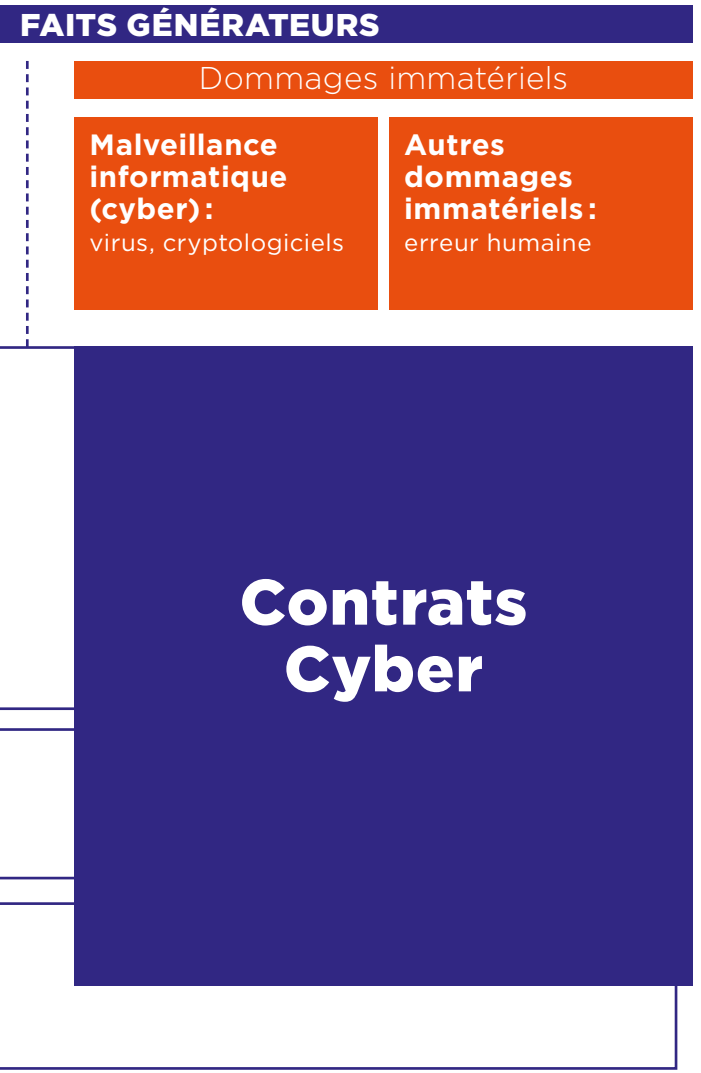
Une matrice simplifiée présente les contrats d'assurance qui peuvent couvrir les conséquences d'un événement « numérique ».

Matrice synthétique

Faits générateurs / conséquences dommageables /



garanties


FAITS GÉNÉRATEURS
Dommages immatériels
Malveillance informatique (cyber) : virus, cryptologiciels
Autres dommages immatériels : erreur humaine
Contrats Cyber

Votre assureur à vos côtés

En matière de risque cyber, votre assureur est là pour vous :

- **Conseiller en matière de prévention**
- **Accompagner dans la gestion de crise post incident**
- **Indemniser en cas de survenance de dommages**

Avec l'aide de votre partenaire assureur, vérifiez le domaine et l'étendue de vos contrats en cours pour savoir si vous êtes correctement couverts en cas de survenance d'un incident informatique, et plus spécifiquement d'une cyber attaque.

Que faire en cas d'incident informatique ?

VIS-À-VIS DE MON ASSUREUR

Contacter sans délai votre partenaire assureur pour déclarer le siniste, il saura vous conseiller et vous accompagner.

Informez-le avant toute décision qui pourrait avoir un impact sur les conséquences de cet incident et sur la gestion de votre dossier de déclaration de sinistre.

VIS-À-VIS DES POUVOIRS PUBLICS

Porter plainte :

L'attaque dont vous avez été victime constitue une infraction aux technologies de l'information et de la communication. Le Code Pénal et le Code Monétaire et Financier définissent ces infractions (se reporter à la page 20 « Sur quel fondement juridique puis-je porter plainte ? »).

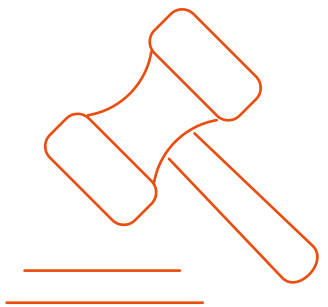
Une plainte doit être déposée dans les plus brefs délais auprès du service territorial de police, de gendarmerie le plus proche de l'entreprise ou par courrier auprès du procureur de la République du Tribunal de Grande Instance de votre ressort géographique.

En cas d'attaque avérée ou même de suspicion d'attaque informatique, l'entreprise victime se doit de récolter des preuves numériques grâce à des constatations techniques. Ces constatations peuvent être complétées par un spécialiste en cybercriminalité nommé par les services de police, lors de leur enquête (se reporter à la bibliographie page 26 « Réagir à une attaque informatique : 10 préconisations »).

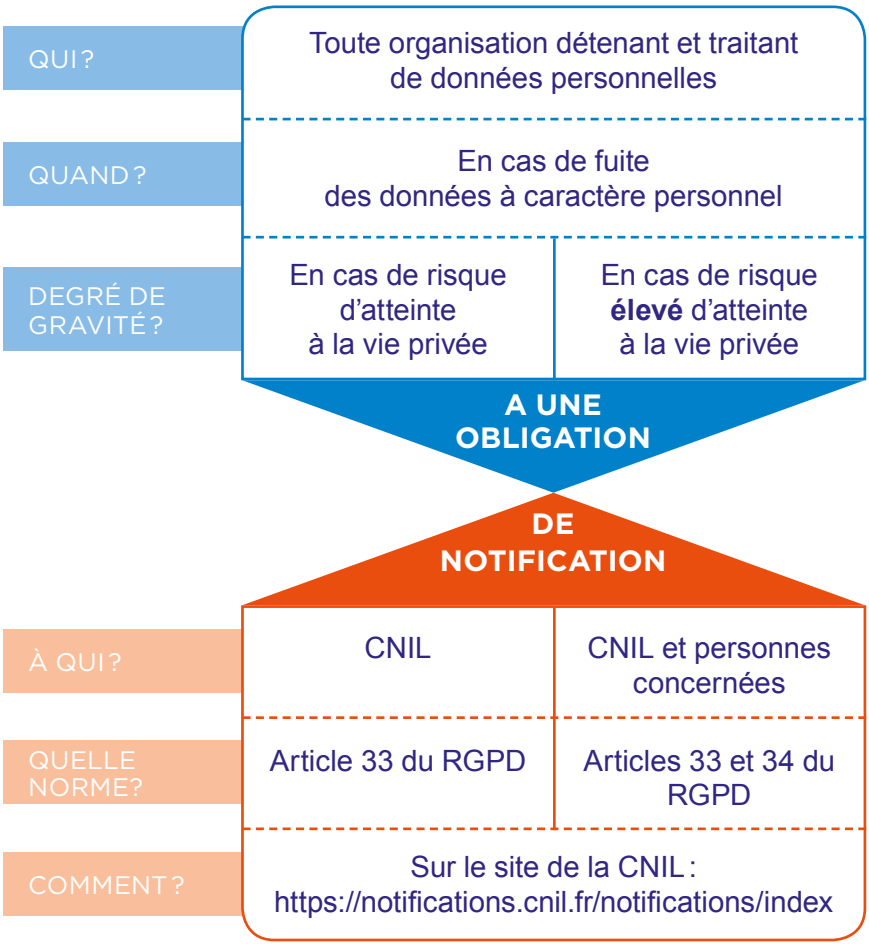
Notifier l'incident :

En cas de fuite des données personnelles, en vertu de l'article 33 du Règlement général sur la protection des données (RGPD), toute organisation traitant de données personnelles* devra le notifier à la Commission Nationale de l'Informatique et des Libertés (CNIL) en cas de risques pour les droits et libertés des personnes, en utilisant le formulaire téléchargeable sur le site www.cnil.fr (voir le schéma de synthèse page suivante). La notification initiale devra être effectuée dans les 72 heures suivant la constatation de la violation, à défaut les motifs du retard devront être exposés dans la notification.

En vertu de l'article 34 du RGPD, dans le cas d'un risque élevé d'atteinte à la vie privée, l'entreprise devra également notifier la violation des données personnelles aux personnes concernées.



* Article 4 du RGPD : une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.



Certaines entreprises sont soumises à des règlementations spécifiques* qui les définissent comme Opérateur d'importance vitale (OIV), Opérateur de service essentiel (OSE) ou fournisseur d'accès internet (FAI).

Lorsque vous êtes sous-traitants de ces entreprises, ces-dernières peuvent vous imposer de renforcer vos mesures de sécurité informatique.

* Loi n° 2013-1168 relative à la programmation militaire et de la directive européenne 2016/1148 transposée par la loi n° 2018-133 du 26 février 2018

Les questions fréquentes

Qu'est-ce qu'une donnée à caractère personnel ?

Conformément à l'article 2 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Quelles sont les attaques les plus fréquentes ?

Les attaques les plus fréquentes sont les dénis de service, les cryptologiciels (de l'anglais *"crypotlockers"*) et rançongiciels (de l'anglais *"ransomwares"*) ainsi que les logiciels malveillants (de l'anglais *"malware"*).

Qu'est-ce qu'un déni de service ?

Une attaque par déni de service (ou attaque par déni de service distribué – de l'anglais DDoS "*Distributed Denial of Service"* – est une forme d'attaque qui consiste à saturer les capacités de traitement d'un système d'information ou d'un site internet à partir d'autres machines préalablement infectées.

Qu'est-ce qu'un cryptologiciel ou rançongiciel ?

Il s'agit d'un programme malveillant qui va crypter les données d'un système d'information. La clé de décryptage est obtenue contre paiement d'une somme, le plus souvent sous forme virtuelle (bitcoins).

Qu'est-ce qu'un logiciel malveillant ?

Les logiciels malveillants sont des programmes qui vont affecter le fonctionnement d'un système d'information. Ils peuvent être désignés sous le nom de virus, vers, chevaux de Troie…

Quels sont les outils et services de surveillance et de détection évoqués en page 9 de ce guide

1 **Les IDS** (Intrusion Detection System) et **SIEM** (Security Information and Event Management) permettent de visualiser en temps réel l'état des composants du système d'information, les journaux d'événements,

ainsi que les flux entrants, sortants et même internes afin de détecter de potentielles attaques ou défaillances.

❷ **Les scanners de vulnérabilités** permettent une approche active via l'utilisation d'outils automatisés permettant l'identification de vulnérabilités sur les composants du système d'information. Cette identification permet de corriger les failles, avant qu'elles ne soient exploitées par une menace.

❸ **Le SOC** est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

Suis-je correctement protégé si mon environnement bureautique est sécurisé ?

Non. Selon les cibles qu'ils visent, les hackers peuvent également s'en prendre à votre informatique de gestion comme la comptabilité, les fichiers du personnel ou encore à votre informatique de process (automates…), voire à vos installations de sécurité et de sûreté.

Quels sont les risques liés au Wifi ou au Bluetooth et plus généralement aux objets connectés ?

Si les données entrantes et sortantes de votre système d'information ne sont pas cryptées avec un niveau de sécurité suffisant, elles deviennent très facilement accessibles notamment via le wifi et le Bluetooth. Les objets connectés augmentent les voies d'accès aux données et aux systèmes d'information de l'entreprise, et donc les failles que des hackers peuvent exploiter.

Qu'est-ce que le "BYOD" et quels sont les risques inhérents à l'utilisation de ces outils ?

BYOD est l'acronyme de *"Bring Your Own Device"* en anglais. Il peut se traduire par « apportez vos appareils personnels ». Cela consiste à utiliser ses équipements personnels pour des usages professionnels. Ce mélange de la sphère personnelle – présumée moins bien protégée et en tout état de cause hors du contrôle de l'entreprise – et de la sphère professionnelle multiplie les risques. Le BYOD augmente les moyens d'accès aux données et aux systèmes d'information de l'entreprise, et donc les failles que des hackers peuvent exploiter.

Quels sont les risques du Cloud ?

Le Cloud computing ou Cloud est l'exploitation de systèmes d'information distants par l'intermédiaire d'un réseau et notamment internet. Il s'agit d'hébergement de données sur des applicatifs distants. Cette externalisation par l'entreprise de données ou de tâches est susceptible de compromettre sa maitrise sur celles-ci. L'entreprise se doit d'analyser les risques de cette externalisation ainsi que les conditions et outils nécessaires pour garantir le niveau de confiance et de sécurité attendu de l'entreprise prestataire.

Sur quel fondement juridique puis-je porter plainte ?

La France possède un arsenal juridique complet dans les domaines liés à la cybercriminalité qui définit notamment des infractions spécifiques aux technologies de l'information et de la communication :

Art 323-1 à 323-7 du Code Pénal :
Les atteintes aux systèmes de traitement automatisé de données (accès ou maintien frauduleux, entrave au fonctionnement, détention de matériel ou logiciel spécifique, groupement formé ou entente établie).

Art 226-16 à 226-20 du Code Pénal :
Les infractions à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (collecte frauduleuse, traitement de données à caractère personnel, usurpation d'identité numérique).

Art. L163-3 à L163-12 du Code Monétaire et Financier :
Les infractions aux cartes bancaires (contrefaçon, falsification de moyens de paiement, détention de matériel ou logiciel spécifique).

Art. 434-15-2 du Code Pénal :
Les infractions au chiffrement (refus de remettre une clé de déchiffrement ou de la mettre en œuvre).

Art. 226-1 à 226-4 du Code Pénal :
Violation de la vie privée par captation à l'aide d'un dispositif technique, divulgation publique d'un enregistrement de la vie privée, conception, importation, location, détention, offre, d'outils de captation de la vie privée et des correspondances.

Qui est l'ANSSI ?

Créée en 2009, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Elle accompagne les administrations, les acteurs économiques et le grand public dans la transition numérique et participe à la protection et à la défense du potentiel économique de la

Nation tant au niveau central qu'au niveau local. Elle est également chargée de la promotion des technologies, de systèmes et de savoir-faire nationaux qui contribuent au développement de la confiance dans le numérique en France et en Europe.

Depuis l'adoption de la Directive Network and Information System Security (NIS), l'ANSSI est l'autorité qui travaille en collaboration avec le Premier Ministre pour désigner les OSE.

Par ailleurs, elle est l'autorité compétente à contacter lorsque les OSE, OIV et FAI sont victimes d'une violation de leurs systèmes d'informations.

Qui est la CNIL ?

Instaurée par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission Nationale de l'Informatique et des Libertés (CNIL) est le régulateur de l'utilisation des données personnelles. Cette autorité administrative indépendante a vocation à s'assurer de la protection et de la bonne gestion des données à caractère personnel en accompagnant les entreprises ainsi que les particuliers dans l'utilisation des nouvelles technologies.

Avec l'adoption du RGPD, la CNIL est l'autorité compétente nationale à contacter en cas de violation de données personnelles.

Pour une régulation harmonisée de l'activité de traitement des données à caractère personnel, la CNIL travaille en collaboration avec ses homologues européens (G29), remplacé par « Le Comité Européen de la Protection des Données (EDPB) » et internationaux.

Qui est CYBERMALVEILLANCE.GOUV.FR ?

Cybermalveillance.gouv.fr, issu de l'ANSSI, est un dispositif gratuit d'assistance aux victimes de cybermalveillance.

Cet organisme regroupe l'ensemble des professionnels du secteur et poursuit trois objectifs principaux :

1. Mettre en relation les victimes (particuliers, entreprises et collectivités territoriales) d'incidents avec des prestataires informatiques qui pourront réparer leurs systèmes ;

2. Mettre à disposition de tous, des outils pédagogiques de prévention des risques numériques ;

3. Mettre en place un observatoire des risques numériques afin de mieux les anticiper, les comprendre et les combattre.

BIBLIOGRAPHIE

Guide d'hygiène informatique de l'ANSSI :
https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

Guide des bonnes pratiques de l'informatique ANSSI/CGPME :
https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/

Réagir à une attaque informatique – 10 préconisations :
https://www.cybermalveillance.gouv.fr/operations/reagir-a-attaque-informatique/

Protection des données personnelles : Risques encourus et assurance, Guide pédagogique édité par la FFA : https://www.ffa-assurance.fr/infos-assures/protection-des-donnees-personnelles-risques-encourus-et-assurance

Rapport, *assurer le risque cyber du Club des Juristes* : http://www.leclubdesjuristes.com/les-commissions/commission-cyber-risk-tome-1-assurer-risque-cyber/

SITES GOUVERNEMENTAUX

Site de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : http://www.ssi.gouv.fr/

Site dédié de la Police :
https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite

Site dédié de la Gendarmerie :
http://www.gendarmerie.interieur.gouv.fr/Zooms/Cybercriminalite

Site du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques CERT-FR :
http://www.cert.ssi.gouv.fr/

Site de la Commission Nationale de l'Informatique et des Libertés (CNIL) : https://www.cnil.fr/professionnel

NORMES ET DOCUMENTS TECHNIQUES

Organisation internationale de normalisation
– Normes ISO série 27000 :
https://www.iso.org/obp/ui/#iso:std:73906:fr ;
– Normes ISO série 27001 :
https://www.iso.org/fr/isoiec-27001-information-security.html ;
– Normes ISO série 27005 :
https://www.iso.org/fr/standard/75281.html

ANSSI – Prestataires de services de confiance qualifiés :
https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/

ANSSI – Prestataire d'audit de la sécurité des systèmes d'informations qualifiés :
https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/

Centre national de prévention et protection (CNPP) : Référentiel D32, Document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique :
https://www.cnpp.com/Boutique-Editions/Referentiels/Referentiels-APSAD/Referentiel-APSAD-D32

Cybermalveillance.gouv.fr :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/

La méthode EBIOS, Risk Manager de l'ANSSI : https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

Fédération Française de l'Assurance

www.ffa-assurance.fr