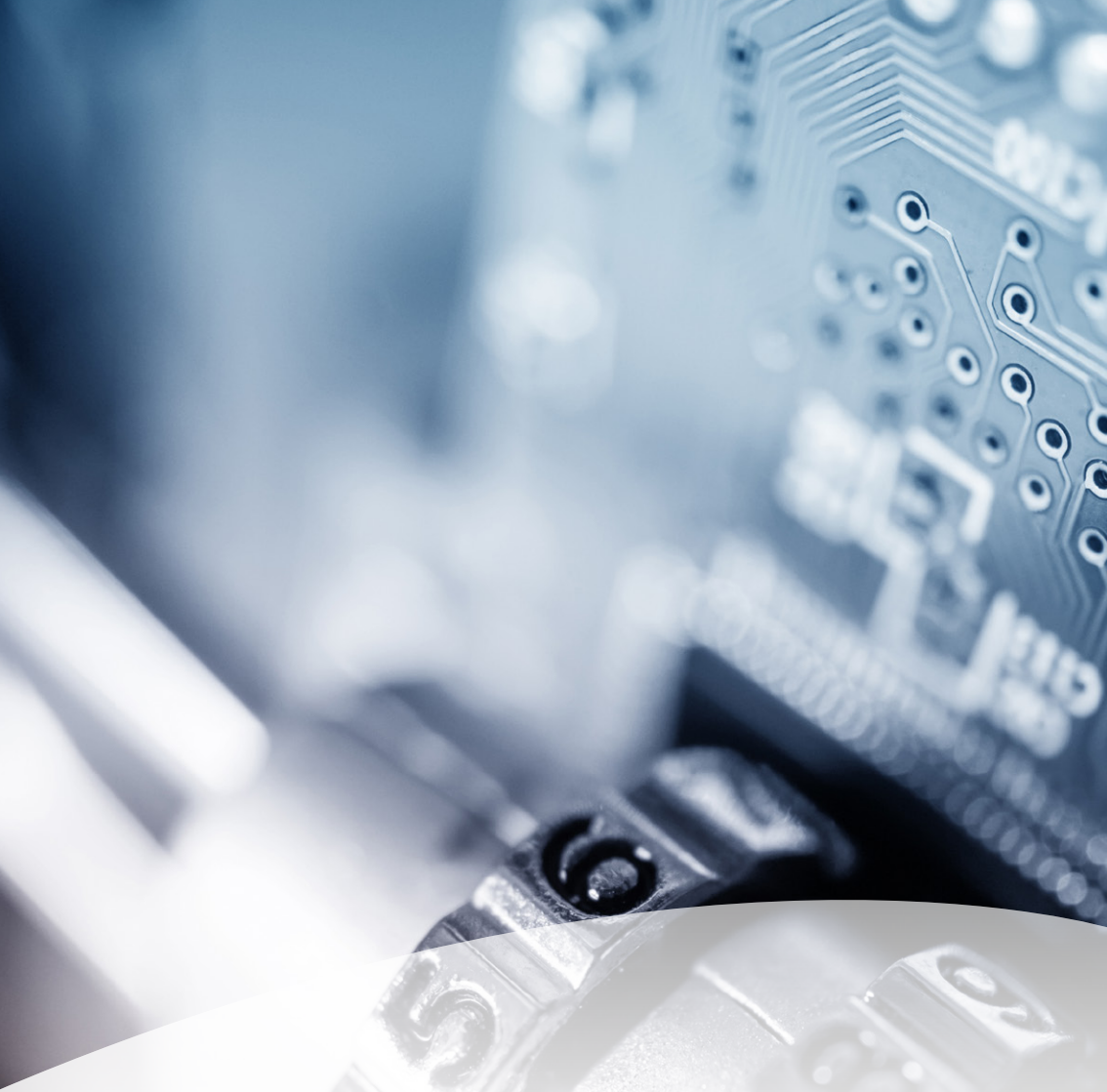


ANTICIPER ET MINIMISER L'IMPACT D'UN CYBER RISQUE SUR VOTRE ENTREPRISE

TPE, PME, vous êtes concernées !

Fédération Française de l'Assurance

Avant-Propos

Se protéger des cyber risques n'est plus une option pour les entreprises, quelle que soit leur taille. L'enjeu économique est vital : il s'agit de préserver vos savoir-faire, vos compétences, vos données sensibles. En un mot, votre compétitivité.

Votre assureur dont le métier est la gestion des risques, est votre partenaire privilégié pour vous accompagner dans la maitrise de ces nouveaux défis .

Vous trouverez dans ce guide les bonnes pratiques à adopter pour anticiper et minimiser l'impact d'un cyber risque sur votre entreprise et lui permettre de poursuivre sereinement son développement.

Bernard SPITZ
Président de la Fédération
Française de l'Assurance

SOMMAIRE

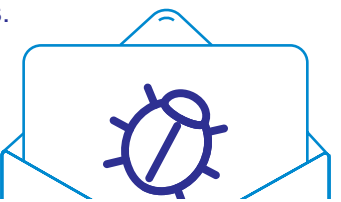
CYBER-RISQUES

Et si cela vous arrivait.

- Un salarié reçoit un courriel supposé de La Poste et clique sur le lien censé lui communiquer le lieu de remise de son colis. En réalité, il télécharge, sans le savoir, un logiciel de cryptage de données. L'ensemble des données de l'entreprise sont alors cryptées et totalement inutilisables. Les pirates informent l'entreprise que pour recouvrer l'accès à ses données elle doit payer une rançon. En contrepartie d'un paiement via un support impersonnel et dématérialisé (bitcoins), la société est censée recevoir en échange la clé de chiffrement utilisée par les cyber-rançonneurs.

- Des hackers exploitent une faille de sécurité du système d'information d'un fournisseur de services de communications électroniques au public. Ils accèdent ainsi aux données de facturation de la base clients et prestataires. Les données revendues à des fraudeurs seront utilisées pour des usurpations d'identité et des détournements de fonds. Le service comptable et commercial de l'entreprise est impacté pendant plusieurs jours. Ces données étant considérées comme des données personnelles, la société doit notifier l'incident à la Commission Nationale de l'Informatique et des Libertés (CNIL) (se reporter à la page 21 « Qui est la CNIL ? »). Elle prend l'initiative d'informer ses clients et est amenée à compenser certains de leurs frais pour monitorer leurs comptes bancaires. Outre la perte de confiance de la part de certains partenaires et clients, l'entreprise et ses dirigeants devront subir les conséquences de la longue enquête administrative qui s'en suivra.

- Un salarié, faisant l'objet d'une sanction disciplinaire, infecte via une clé USB un équipement de contrôle du site industriel qui l'emploie. Cette attaque du système d'information provoque d'importantes nuisances au voisinage.
  Les riverains se plaignent aux autorités. L'entreprise doit engager des frais de détection et de décontamination de son système d'information et mobiliser des ressources internes pour gérer les conséquences de l'événement. Mais les relations entre l'entreprise et les autorités en seront durablement affectées et des projets de développement retardés.



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

- Mes données clients sont-elles susceptibles d'intéresser un tiers, la concurrence ?
- Mon système d'information est il correctement protégé ?
- En cas de cyber attaque, mon entreprise serait-elle affectée si je ne pouvais plus accéder à mon système d'information ou à mes données ? Une baisse significative d'activité est-elle à craindre ? Un arrêt total, mettant en péril l'existence même de mon entreprise, peut-il être envisagé ?
- Ai-je mis en place un plan de continuité d'activité en cas d'indisponibilité de mon système d'information ou de mes données ?
- Qui contacter en cas de cyber attaque pour gérer cette crise ?

Si vous n'avez pas de réponse satisfaisante à ces questions, **vous êtes vulnérables**.

Si vous êtes vulnérables, **vous devez vous protéger …**

… et **vous assurer pour** le cas où un hacker parviendrait à contourner vos protections.

Protéger mon entreprise.

La sûreté informatique de votre entreprise 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.

Ce process doit être porté par une personne de l'entreprise, clairement identifiée en charge de la mise en place et du suivi de cette politique de management du cyber risque.

Cette politique doit reposer sur 3 piliers :

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

Exemples de bonnes pratiques et d'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 bons réflexes.

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, ce sont aussi vos sous-traitants et vos prestataires, qui doivent également être sensibilisés et formés pour éviter qu'ils deviennent les maillons faibles de votre protection face aux risques cyber.

FACTEURS ORGANISATIONNELS :

La prévention de votre entreprise passe, notamment, par :

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

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

Pour éviter qu'ils soient facilement usurpés, vos mots de passe doivent être individualisés, secrets, robustes (complexes) et régulièrement changés. Il est donc utile de définir un niveau minimal de sécurité tel que 8 caractères mélangeant majuscules, minuscules et chiffres.

2. Une formation adaptée de votre personnel et de vos partenaires :

La totalité de vos collaborateurs, dont les CDD, stagiaires, alternants compris, doit être sensibilisée aux cyber risques et formée pour s'en prémunir.

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,
- Élaborer des règles de consultation des mails et pièces jointes douteux (liens hypertextes ou inexplicables, 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 des logiciels opérationnels de gestion, de process et de production :

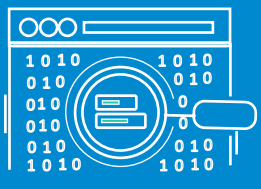
Les failles de vos logiciels sont autant de chemins d'accès pour des intrusions malveillantes. Au fur et à mesure de leurs identifications, ces failles doivent être corrigées.

OUTILS DE PROTECTION :

La protection de votre entreprise 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 :

ANTI-VIRUS / 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 DÉTECTION COMPORTEMENTALE

D'autres intrusions malveillantes non stoppées par les outils de filtrage ne peuvent être détectées que par des outils de détection comportementale.

Ces outils analysent le comportement des téléchargements ayant passé l'anti virus, afin de détecter ceux qui ont des actions suspectes (black list des logiciels malveillants connus). Comme par exemple les cryptologiciels (de l'anglais cryptolockers) lorsqu'ils interrogent et écrivent sur un grand nombre de répertoires de l'ordinateur.

OUTILS DE FILTRAGE

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

ANTICIPATION DE LA GESTION DE CRISE : OUTILS DE RÉSILIENCE

La capacité de l'entreprise à redémarrer rapidement après une attaque s'anticipe, notamment, sur les deux 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 :

- Qualifier vos données, systèmes d'exploitation et applications critiques en termes de données confidentielles ou personnelles.
- Mettre en place une procédure de gestion de crise en cas de survenance d'une attaque.
- Nommer des collaborateurs (responsables, experts et communicants) mobilisables à tout moment et sans délai, qui auront 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 entreprise.

Assurer mon entreprise.

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

- **Les contrats de dommages aux biens** (multirisques et pertes d'exploitation) couvrent généralement les conséquences (frais de recherche de la cause, réparations, pertes d'exploitation consécutives…) des accidents (incendies, événements naturels, …), des erreurs humaines (imprudence, négligence, …) ou des actes de malveillance (vol, sabotage, …) qui entraînent des dommages matériels à vos bâtiments et/ou à leur contenu.

- **Les contrats cyber** couvrent généralement les mêmes conséquences (frais de recherche, de reconstitution des données, pertes d'exploitation consécutives…) mais qui font suite à des événements d'origine informatique sans dommage matériel, qu'ils soient de nature :

  - **Accidentelle**, notamment dûs à une erreur humaine.
  - **Volontaire**, notamment par des actes de malveillance tels que des virus, accès illicite à des données personnelles ou confidentielles, cryptologiciel, attaque par déni de service (de l'anglais Distributed Denial of Service ou DDoS), ou toute intrusion numérique non autorisée en vue de détourner des données ou des fonds.

En complément, les contrats cyber peuvent couvrir également :

- Les frais de notification suite à atteinte, vol ou extraction de données personnelles et/ou confidentielles qui vous auraient été confiées tels que les frais engagés pour la déclaration d'incident au régulateur — la CNIL pour la France — les frais d'information et de prévention aux titulaires des données détournées et les frais induits par l'enquête administrative.
- Des frais de gestion de crise, comme des frais de communication et/ou de préservation de la réputation et de l'image de la société,
- Des frais de consultants spécialisés en vue de faire cesser une cyber-extorsion.

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

- **Les contrats de responsabilité civile** couvrent votre responsabilité pour les dommages causés aux tiers (clients, voisins, salariés…) que ces dommages soient corporels, matériels et/ou immatériels. Ces contrats peuvent couvrir également les frais de retrait et les frais de dépose-repose.

- Certains contrats de responsabilité civile peuvent exclure ou limiter la garantie de votre responsabilité vis-à-vis des tiers pour les dommages purement immatériels lorsqu'ils sont la conséquence d'une malveillance informatique. Cette même garantie peut être couverte dans un **contrat cyber.**

Pour assurer mon risque de fraude :

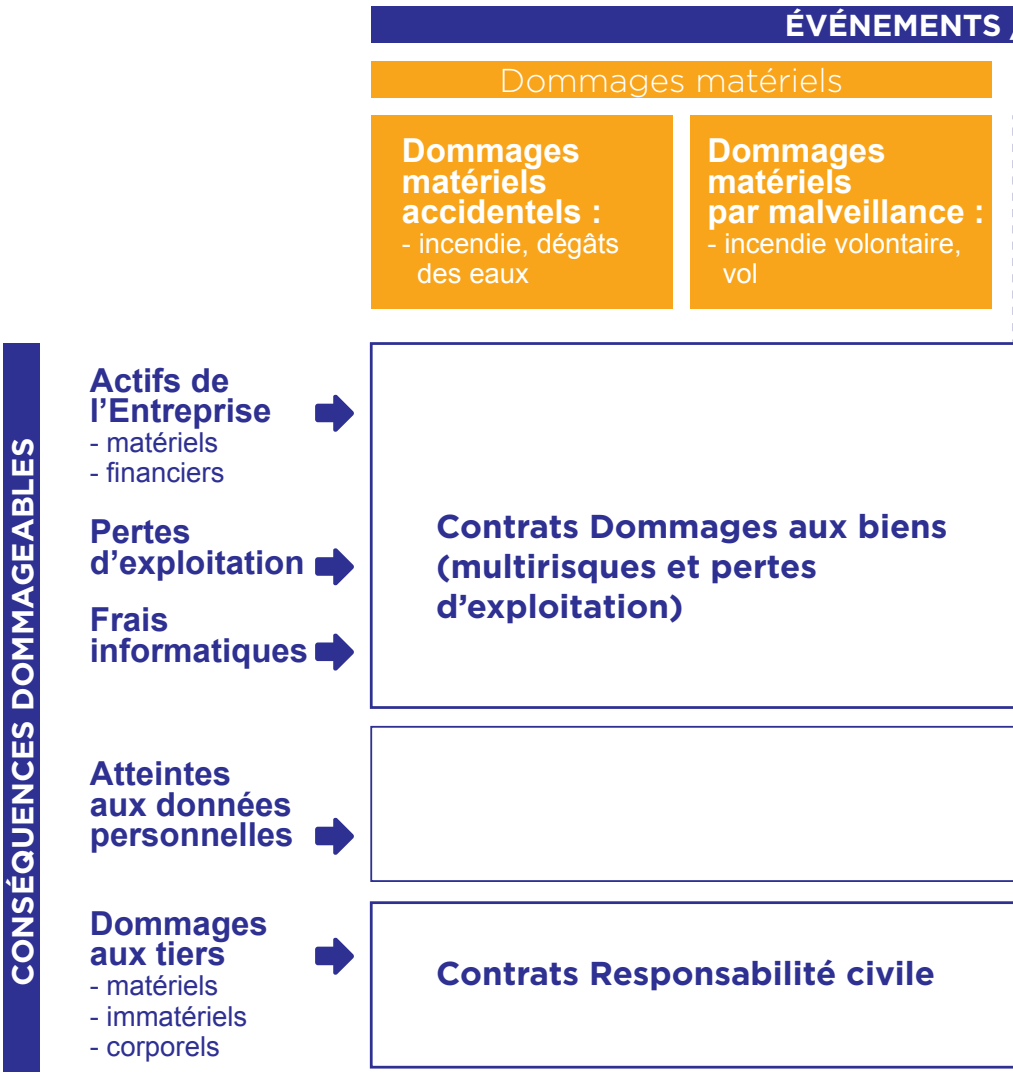
- **Les contrats contre la fraude** couvrent géné-ralement les pertes financières causées par des fraudes, par des détournements de fonds (extorsions, abus de confiance, escroqueries…) ou par certains actes de malveillance informatique.

- Cette même fraude consécutive à des actes de malveillance informatique peut aussi être couverte en extension dans un **contrat cyber.**

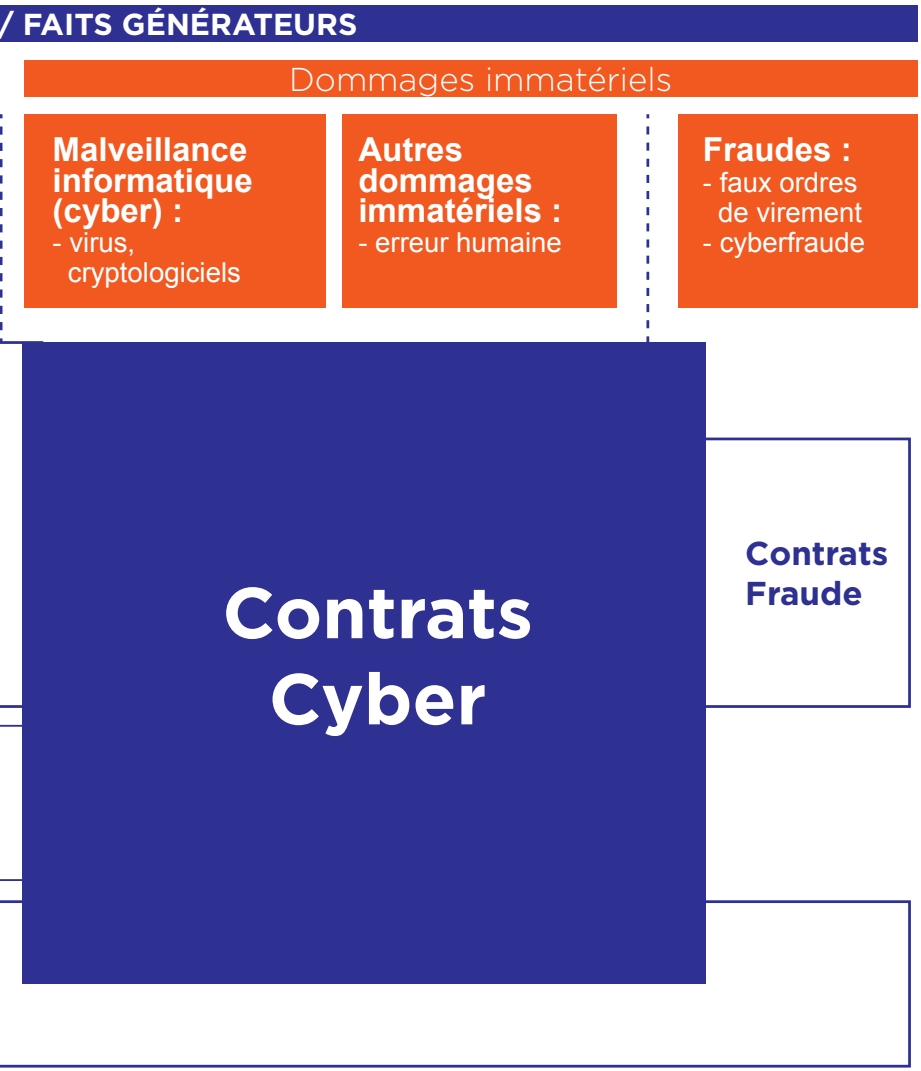
Une matrice simplifiée présente les contrats d'assurance qui peuvent couvrir les conséquences d'un évènement «numérique».

Matrice synthétique

Faits générateurs / conséquences dommageables /



/ garanties


/ FAITS GÉNÉRATEURS
Dommages immatériels
Malveillance informatique (cyber) :
- virus, cryptologiciels
Autres dommages immatériels :
- erreur humaine
Fraudes :
- faux ordres de virement
- cyberfraude
Contrats Cyber
Contrats Fraude

Que faire vis-à-vis de mon assureur ?

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

Que faire en cas d'incident informatique ?

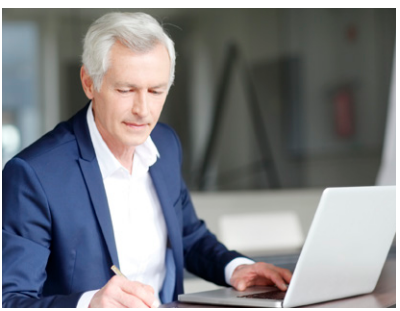
VIS-À-VIS DES POUVOIRS PUBLICS :

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 22 « Réagir à une attaque informatique : 10 préconisations »).



Notifier l'incident :

En cas de violation des données personnelles, l'obligation de notification à la Commission Nationale de l'Informatique et des Libertés (CNIL) est issue de l'article 34 bis de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle s'adresse aux fournisseurs de services de communications électroniques au public. L'intéressé doit être averti en cas de risque d'atteinte à ses données personnelles ou à sa vie privée.

Cette obligation de notification sera étendue à l'ensemble des entreprises ayant des activités de traitement de données à caractère personnel à compter de mai 2018[1].

En cas d'atteinte au système d'information, la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 prévoit à l'article 22 que l'incident doit être notifié auprès du Premier Ministre et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) (se reporter à la page 21 « Qui est l'ANSSI? ») pour les opérateurs d'importance vitale.

Cette obligation sera étendue aux entreprises qualifiées « d'opérateur de services essentiels » ou de « fournisseur de services numériques » lors de la transposition de la directive (UE) 2016/1148 relative à la sécurité des réseaux et systèmes d'information dans l'Union Européenne (SRI) d'ici mai 2018[2].

[1] Date d'application au sein de l'Union européenne du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)

[2] Date limite pour la transposition par les Etats membres de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (NIS).

			AUJOURD'HUI	DEMAIN (mai 2018)
En cas de violation des donnees à caractère personnel	**OBLIGATION DE NOTIFICATION**	**Pour qui ?**	**Pour les fournisseurs de services de communications électroniques au public** (Loi Informatique et libertés 1978)	**Pour toutes les entreprises ayant des activités de traitement de données** (Règlement européen « RGPD » 2016/679)
		À qui ?	À la CNIL et à l'intéressé	À l'autorité compétente et à l'intéressé
En cas d'atteinte au système d'information		**Pour qui ?**	**Pour les opérateurs d'importance vitale (OIV)** (Loi de programmation militaire 2014 -2019)	**Pour les opérateurs de services essentiels et fournisseurs de services numériques** (Directive européenne « NIS »2016/1148)
		À qui ?	Au Premier ministre et à l'ANSSI	À l'autorité compétente

VIS-À-VIS DE MON ASSUREUR ?

Contacter sans délai votre partenaire assureur, il saura vous conseiller et vous accompagner.

En tout état de cause, 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.

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…

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-faires nationaux qui contribuent au développement de la confiance dans le numérique en France et en Europe.

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.

Pour une régulation harmonisée de l'activité de traitement des données à caractère personnel, la CNIL travaille en collaboration avec ses homologues européens (G29) et internationaux.

BIBLIOGRAPHIE :

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

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

Réagir à une attaque informatique -10 préconisations :
http://www.vaucluse.cci.fr/wp-content/uploads/2016/09/2016-10-preconisations-face-cybercriminalite.pdf

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 :
http://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

Site d'Interstats : des statistiques publiques sur l'insécurité et la délinquance :
http://www.interieur.gouv.fr/Interstats/Actualites

NORMES ET DOCUMENTS TECHNIQUES

Organisation internationale de normalisation – Normes ISO série 27000 : http://www.iso.org/iso/fr/home/standards/management-standards/mss-list.htm

Centre nationale de prévention et protection (CNPP) – Référentiel CNPP 4032 Cyber sécurité : Guide pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique : http://www.cnpp.com/Boutique-Editions/Referentiels/Referentiels-CNPP/Referentiel-CNPP-4032

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

Fédération Française de l'Assurance

www.ffa-assurance.fr