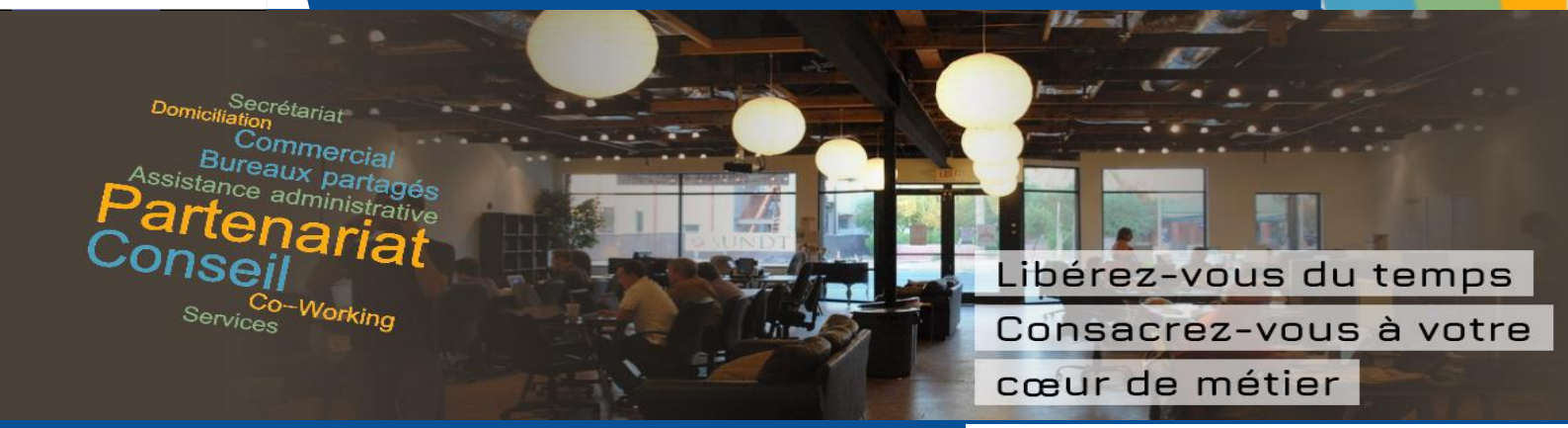
Caen Conseil



Newsletter n° 3

RISQUE INFORMATIQUE – CYBERCRIMINALITE

Quel impact dans les PME / TPE et quelle évolution ?

En 2016, 80 % des entreprises ont été victimes d'une cyberattaque, et cela évolue régulièrement !

Les entreprises ont connu voilà quelques années, la transition Informatique. A présent elles sont inexorablement soumises à l'évolution Numérique et à son importance de plus en plus forte pour toutes les fonctions vitales de leur fonctionnement régulier.

Cette évolution se traduit, bien évidemment, par le développement toujours plus performant de moyens techniques tels que : les ordinateurs de nouvelle génération et leur virtualisation, les robots et l'intelligence artificielle, les réseaux de télécommunication toujours plus rapides et plus performants, mais aussi par l'impact très fort pour les utilisateurs, internes et externes, des transferts de données via des espaces de stockage, de l'utilisation des messageries, et surtout des smartphones avec leurs multiples applications.

Bien naturellement tout cela a pour conséquences directes : L'évolution permanente du *Risque Informatique* et l'apparition de la **Cybercriminalité**.

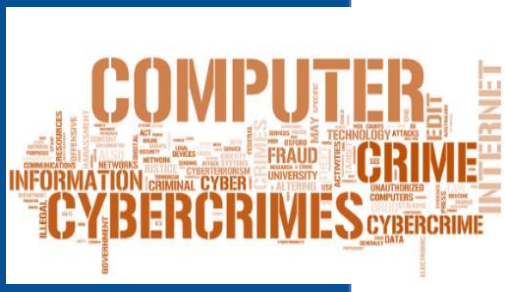
Ces 2 points sont distincts, mais fortement complémentaires, même si aujourd'hui la **Cybercriminalité** constitue l'un des facteurs majeurs des dangers liés à l'utilisation des S.I.

Entendons par *Risque Informatique*, toute action accidentelle ou malveillante, susceptible de mettre en danger le fonctionnement régulier d'une entreprise, où de toute activité professionnelle.

Cela peut se traduire par :

- Un arrêt de fonctionnement du S.I (incident technique, coupure de courant, inondation, …)
- Une perte de fichiers conséquente à une fausse manipulation, ou un incident technique, …
- Une copie de données sensibles pour une utilisation externe, ou plus précisément un vol de données.
- Une impossibilité de fonctionnement liée à une absence de sauvegarde,
- …

Caen Conseil vous souhaite de belles fêtes de fin d'année



La **Cybercriminalité** produira les mêmes effets d'impossibilité de fonctionnement régulier pour l'entreprise, mais très largement amplifiés, parce que toujours générés de façon volontaire et régulièrement accompagnés de menaces techniques et/ou financières afin de nuire gravement à la cible visée. Cette Cybercriminalité se manifeste de multiples façons (spyware, phishing, ransomware, ransomhack, …) sans cesse renouvelées. Les actions malveillantes pouvant être activées au travers de tout élément connecté : ordinateur, tablette, smartphone, réseaux sociaux, ...

Selon une récente étude*, il a été constaté une très nette évolution de la **Cybercriminalité** entre 2016, année au cours de laquelle 80% des entreprises avaient été victimes d'une cyberattaque, et 2017 où la proportion des cibles atteint 92%. Le temps nécessaire au rétablissement d'une activité normale, suite à une cyberattaque peut demander plusieurs jours. Il apparaît que 9 entreprises sur 10 ont été victimes d'attaques susceptibles de mettre en danger leur fonctionnement : 19 millions de Français (particuliers) ont été touchés par une cyberattaque en 2017 !

Des actions de protection, voire des lois, peuvent être mises en place de façon nationale ou internationale, mais cela n'arrêtera pour autant, l'évolution de la Cybercriminalité. Depuis plusieurs mois les TPE/PME sont soumises à la nouvelle protection des données à caractère personnel : la R.G.P.D, mise en place par la C.N.I.L. Si cette réglementation impose aux entreprises des règles de protection de certaines données enregistrées, elle a, en contrepartie donné quelques idées aux organismes de cybercriminalité pour récupérer des données sensées être protégées, et conditionner leur restitution à quelque rançon.

Alors comment se protéger contre tous ces risques, quasi permanents et en permanente évolution, qui menacent les données et le bon fonctionnement des entreprises ?

Les actions sont assez nombreuses et doivent être menées selon un ordre bien défini et une méthodologie précise. Ce sujet, vaste et relativement compliqué, fera l'objet d'un document complémentaire permettant de définir le Plan d'action nécessaire. Cependant il ne semble pas inutile de rappeler les premiers principes de base que toute entreprise doit appliquer de façon régulière. Cela concerne l'information de tous les utilisateurs, la communication et la mise en application des règles simples telles que :

- ne pas laisser son poste de travail connecté 24/24,
- utiliser des mots de passe différents selon les applications utilisées et les changer suffisamment souvent, - sauvegarder ses fichiers importants,
- ne pas ouvrir de mails dont l'origine semble douteuse ou inconnue,
- ne pas échanger de données entre son smartphone et son poste de travail sans autorisation et vérification préalable, …

* Etude du Club des Experts de la S.I et du Numérique - Etude Norton / Symantec

Caen Conseil

205 Rue de Bayeux
14000 CAEN
02 31 73 88 55
secretariat@caenconseil.com
www.caenconseil.com