

# Les secteurs à risque courants dans l'industrie automobile

**LE SAVIEZ-VOUS?**  
**En 2017, une brèche de données moyenne touchait plus de 24 000 dossiers.** <sup>1</sup>



Avec autant de documents exposés à des risques, les concessionnaires automobiles de toute l'Amérique du Nord doivent être conscients de leurs secteurs vulnérables.



## **L'absence de politiques :**

Les concessionnaires automobiles ont été plus lents à suivre l'évolution de la technologie de l'information et à se prémunir contre ses dangers.<sup>2</sup> Les organisations doivent avoir des politiques officielles en matière de cybersécurité, des plans d'intervention en cas d'incident et des procédures de sauvegarde et de restauration.



## **Les employés :**

Les employés peuvent représenter l'un des plus grands facteurs de risque. Souvent, une attaque survient lorsqu'un employé peu méfiant ouvre un courriel contenant un virus malveillant. Une récente étude révèle que 54 % des petites et moyennes entreprises (PME) ont déclaré que les employés négligents sont la cause des cyberincidents.<sup>3</sup>



## **Les arnaques en ligne :**

Les « hameçonneurs » tentent de convaincre le destinataire de se connecter à un système malveillant ou de télécharger un logiciel malveillant. Dans une récente alerte de sécurité, une entreprise de technologies automobiles mettait en garde contre des pirates qui inséraient des logiciels malveillants dans des messages sur les réseaux sociaux conçus pour inciter les employés à cliquer sur le message.



## **L'interconnectivité :**

Les concessionnaires automobiles sont interconnectés aux fabricants de voitures, aux fournisseurs et aux commerçants. Une recherche démontre que de nombreuses brèches sont liées à des tierces parties.<sup>4</sup>



## **« Apportez vos appareils personnels »**

Les employés conservent souvent sur leurs propres appareils mobiles ou ordinateurs portatifs des renseignements permettant d'identifier une personne. Les appareils personnels sont l'un des outils les plus fréquemment utilisés par les employés malveillants et par les pirates informatiques dans les cas de vol de données.



## **Le manque de personnel en sécurité informatique :**

Une étude récente<sup>5</sup> a démontré que les PME ont habituellement très peu d'employés spécialisés en sécurité informatique disponibles pour s'occuper des questions de sécurité. Environ 80 % des entreprises comptant de 100 à 500 employés ont deux employés ou moins spécialisés en sécurité informatique.



## **L'équipement obsolète :**

De nos jours, la technologie tombe rapidement en désuétude. L'équipement existant peut accroître la vulnérabilité d'un concessionnaire automobile aux attaques.



## 3 conseils pour protéger votre entreprise



### Repérez tous les secteurs de risque potentiels.

Effectuez une inspection de vos bureaux. Signalez tous les risques que vous voyez et prenez des mesures pour les atténuer. Cette inspection vous permettra de découvrir les points faibles de votre entreprise et de renforcer votre stratégie en matière de sécurité de l'information afin de protéger vos données.



### Mettez en place des politiques sur la sécurité des lieux de travail.

En établissant des politiques exhaustives, comme une politique de tout déchetage et une politique de bureau rangé, vous incitez vos employés à réfléchir avant d'agir lorsqu'ils sont au travail. Ils seront ainsi poussés à se conformer aux règles et à protéger vos données.



### Créez une culture de sécurité totale.

En adoptant une approche descendante et en intégrant la sécurité de l'information dans l'ensemble de votre entreprise, vous ferez en sorte que la culture de sécurité totale fasse partie intégrante du quotidien de vos employés. Par le fait même, ceux-ci seront amenés à considérer d'un œil neuf la destruction sécuritaire des renseignements confidentiels.

**Sources:**

1. 2017 Cost of Data Breach Study, Ponemon Institute, 2017
2. 6 Steps to Prevent Hacking at Your Dealership, Dealer Marketing Magazine, août 2017
3. 2017 State of SMB Cybersecurity Report, Keeper Security et Ponemon Institute, 2017
4. The Third Party Data Breach Problem, Digital Guardian, juillet 2017
5. IT Security at SMBs: 2017 Benchmarking Survey, Cyren, 2017

Apprenez-en davantage sur la sécurité de l'information dans l'industrie automobile :

**1 877 227-5986 | [shredit.com/auto](https://shredit.com/auto)**

Shred-it® est une solution Stericycle. © 2018 Shred-it International. Tous droits réservés.

