

# Les cybercrimes

## et les entreprises canadiennes, 2017

Les entreprises ont dépensé

**14 milliards de dollars**

pour prévenir et détecter les incidents de cybersécurité, et pour se rétablir de ces incidents.



**8 milliards de dollars**

pour les salaires des employés, des consultants et des entrepreneurs

**4 milliards de dollars**

pour l'achat de logiciels de cybersécurité et de matériel informatique connexe

**2 milliards de dollars**

pour la mise en place d'autres mesures de cybersécurité



### Raisons invoquées par les entreprises pour investir dans la cybersécurité

**68 %** de la protection des renseignements personnels

**41 %** de la prévention de la fraude et du vol

**31 %** de la prévention de l'interruption des services opérationnels

**21 %** des entreprises ont été touchées par un incident de cybersécurité. En moyenne, ces dernières ont vécu une période d'indisponibilité de **23 heures**.



Taille de l'entreprise

**Grande**  
(250 employés et plus)

**Moyenne**  
(50 à 249 employés)

**Petite**  
(10 à 49 employés)

Entreprises touchées par un incident de cybersécurité

**41 %**

**28 %**

**19 %**

Période d'indisponibilité

**29 heures**

**24 heures**

**22 heures**



Les incidents de cybersécurité provoqués par les cybercriminels ont été faits dans l'intention

de voler de l'argent ou de demander une rançon

**38 %**

d'accéder à des zones d'accès non autorisées

**26 %**

de voler des renseignements personnels ou financiers

**23 %**

de perturber ou de dénaturer l'entreprise ou sa présence sur le Web

**22 %**

Entreprises touchées par un incident de cybersécurité

