

## Protection des protecteurs : L'industrie de l'assurance se tourne vers des experts en sécurité pour obtenir des conseils

Les organisations d'assurance sont connues pour stocker de grandes quantités de renseignements personnels identifiables (PII) sur leurs titulaires de police, ce qui en fait une cible pour la cybercriminalité. Et, par rapport aux autres industries sondées, l'assurance s'en vient à l'égard de ceux qui ont subi une violation de données.



**75 %** DE  
**ORGANISATIONS D'ASSURANCE**

J'ai déjà fait l'expérience d'une violation de données

**65 %** DE  
**ORGANISATIONS D'ASSURANCE**

ont enquêté sur une atteinte à la protection des données survenue au cours des 12 derniers mois

### Les organisations d'assurance comprennent qu'il est important d'être préparé

**44 %**

La sécurité de l'information de l'État est très importante pour leur entreprise

**39 %**

Croire qu'une violation de données serait coûteuse\*

**43 %**

Sentir une violation de données aurait un impact majeur sur leur réputation

**84 %**

Embauche d'un expert en sécurité tiers pour évaluer les pratiques de sécurité

\* En termes d'argent et de temps pris pour corriger la situation.

## Les organisations d'assurance sont plus préoccupées par les documents laissés à l'écart

Les compagnies d'assurance qui ont subi une violation comprennent l'importance de détruire des documents sensibles lorsqu'ils ne sont plus nécessaires pour améliorer les processus commerciaux et protéger les renseignements sensibles contre tout accès non autorisé. Pourtant, la majorité (85 %) des compagnies d'assurance interrogées sont préoccupées par le fait que les employés laissent du matériel confidentiel sur leur bureau. Les organisations d'assurance doivent revoir leur stratégie de protection des données contre les violations de données physiques, car la plupart d'entre elles ont signalé ne pas avoir de service de déchiquetage de papier.

### Politiques et stratégies de protection

- |   |  |  |
|---|--|--|
| <b>50 %</b> ➤ Utiliser une politique sur la sécurité des renseignements | <b>25 %</b> ➤ Effectuer une vérification régulière de l'infrastructure | <b>6 %</b> ➤ Avoir un service de déchiquetage papier pour se protéger contre les violations de données |
| <b>90 %</b> ➤ Avoir une police d'assurance cybernétique                 | <b>13 %</b> ➤ Effectuer des évaluations de vulnérabilité               |  |

### Plan d'intervention

- |  |   |
|--|---|
| <b>25 %</b> ➤ Avoir un plan d'intervention | <b>49 %</b> ➤ A pris environ un mois pour résoudre la plus récente violation de données |
|--|---|