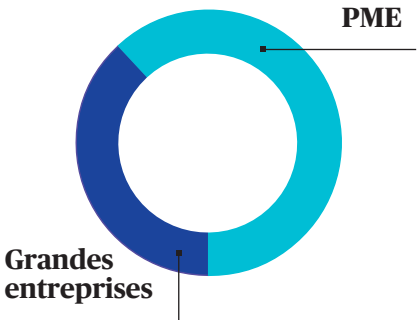
# **L’inévitabilité des cyberattaques** La menace que les petites et moyennes entreprises (PME) ne peuvent pas ignorer

CHUBB®

## Table des matières


## Cibles de cybercriminalité




62 % des cibles cybercriminelles étaient des PME

Depuis plusieurs années, les cyberattaques contre de grandes entreprises, des gouvernements, des universités, des États - voire des pays - sont devenues monnaie courante.

Bien que les incidents à grande échelle retiennent l'attention des médias, les données révèlent que les cybercriminels s'intéressent de plus en plus aux petites entreprises. En fait, 62 % des cibles cybercriminelles étaient des petites et moyennes entreprises (PME), selon Small Biz Trends[1]. Et tout prouve que cette tendance à cibler les PME va s'accentuer.

Pourquoi les petites entreprises sont-elles ciblées par les cybercriminels? C'est probablement parce que les cyberpirates savent que les dirigeants de PME négligent la cybersécurité parce qu'ils la croient, à tort, hors de prix, ce qui les rend vulnérables.

## Le déni des PME

Les cyberattaques contre les PME sont peu rapportées dans les médias. Ces crimes ont donc tendance à passer inaperçus, et les petites entreprises peuvent alors ne pas saisir l'étendue réelle du risque.

Compte tenu de la cadence des changements opérationnels, les PME sont plus nombreuses à adopter la voie du numérique pour éviter de se laisser distancer par la concurrence. Pourtant, cette évolution complexe, mais nécessaire, accroît tout autant leur vulnérabilité à la cybercriminalité.

La cybercriminalité est peu risquée pour les criminels. La même technologie qui améliore l'efficience des entreprises ouvre la voie à une cyberexploitation des failles et des réseaux par intervention rapide, peu coûteuse et anonyme.

Malheureusement, les dirigeants de PME sont mal informés sur la protection contre ces risques et pensent que la possibilité d'une cyberattaque est relativement infime. C'est sur cette naïveté que misent les cybercriminels qui déploient de nombreuses stratégies, dont celles-ci.

Cyber Index[SM2] de Chubb révèle que le coût moyen pour se remettre d'un cyberincident est de 400 000 $.

- **Détournement d'un compte de courrier électronique** - Après avoir accédé à un compte de courrier électronique d'une agence immobilière, un cybercriminel a convaincu un client de l'agence de virer 300 000 $ dans un compte bancaire frauduleux.
- **Fraude par rançongiciel** - L'employé d'un organisme à but non lucratif a accidentellement consulté un site Web malveillant au travail. Le serveur partagé de l'organisme a été infecté par un virus de chiffrement des fichiers. Les cybercriminels ont alors tenté d'extorquer l'organisme sous la menace de publication des documents volés.
- **Fraude par hameçonnage** - Un employé de la comptabilité d'une agence des services sociaux a reçu un courriel d'apparence légitime lui demandant de transmettre les formulaires W-2 d'employés, actuels et anciens, ouvrant ainsi la voie à une usurpation d'identité grâce aux renseignements recueillis.
- **Vol d'ordinateur** - Une petite entreprise de soins de santé s'est fait voler un ordinateur portable, en plein jour, dans lequel étaient stockées les données salariales des employés. L'ordinateur n'a jamais été récupéré.

Vol d'appareils, rançongiciel, hameçonnage ou accès prohibé, les cybercriminels peuvent désormais atteindre l'information sensible par l'extérieur comme par l'intérieur. La technologie facilite la cybercriminalité qui, somme toute, est devenue peu risquée.

### La fatalité de la hausse des cyberattaques chez les PME

Cyber Index[SM2] de Chubb révèle que le coût moyen pour se remettre d'un cyberincident est de 400 000 $.. Cette somme peut signer l'arrêt de mort d'une PME. Le coût très élevé de la remise sur pied d'une entreprise et du rétablissement de sa réputation est d'autant plus déconcertant que ces événements sont très fréquents. Un rapport du FBI3 indique que 4 000 cyberincidents se sont produits tous les jours depuis le 1er janvier 2016, soit une hausse de 300 % par rapport à l'année précédente.

### La protection des PME contre les cyberattaques

Il y a une lueur d'espoir, malgré ces statistiques. Selon Cyber IndexSM, de Chubb, la plupart des cyberincidents peuvent être évités. Mentionnons la perte ou le vol d'appareils, les erreurs de programmation, l'hameçonnage et le non-respect des politiques des entreprises. Cela signifie que les PME peuvent contrer de nombreuses menaces en adoptant les mesures préventives suivantes.

1. **Dressez un plan d'intervention** et investissez dans les ressources pour mener à bien ce plan.

a

### De simples mesures de protection

1. Dressez un plan d'intervention.
2. Mettez un gestionnaire de mots de passe sécurisé à la disposition de vos employés.
3. Sensibilisez vos employés.
4. Installez un bon antivirus.
5. Tenez à jour vos systèmes d'exploitation et vos applications.
6. Protégez vos réseaux.
7. Souscrivez une cyberassurance complète.

Depuis le 1er janvier 2016, 4 000 cyberincidents se produisent chaque jour.

2. **Mettez un gestionnaire de mots de passe sécurisé à la disposition de vos employés** pour la gestion facile et en toute sécurité des identifiants.

3. **Sensibilisez vos employés** à la cybercriminalité et déployez des logiciels capables de réduire les attaques de piratage psychologique comme l'hameçonnage.

4. **Installez un bon antivirus** et tenez-le à jour.

5. **Tenez à jour vos systèmes d'exploitation et vos applications** pour maintenir la prise en charge par le fabricant.

6. **Protégez vos réseaux** par routeur sécurisé à l'interne et réseau privé virtuel (VPN) à l'externe.

En plus de ces six mesures préventives, les entreprises devraient envisager la souscription d'une cyberassurance complète. En fait, de nombreuses cyberassurances soutiennent les services et les ressources énumérés aux présentes. Outre les services intégrés d'atténuation des sinistres pour réduire le risque d'être pris pour cible, une cyberassurance comprendra très certainement des services d'intervention en cas de cyberattaque, notamment, les services d'une équipe d'experts dans les domaines du droit, de la criminalistique informatique, de la notification, des centres d'appels, des relations publiques, des services-conseils en fraude, de la surveillance du crédit et de la récupération de l'identité.

Et, bien entendu, c'est l'assureur qui supportera le risque financier après un cyberincident.

### La cyberassurance des PME en action

Vous vous souvenez des exemples de cybercriminalité que nous avons évoqués précédemment? Heureusement, les quatre entreprises avaient souscrit une cyberassurance bien avant les cyberincidents dont elles ont été victimes. Les polices ont atténué les sinistres et favorisé la reprise des activités des PME, tout en les blindant contre de futures attaques.

- **Détournement d'un compte de courrier électronique** – L'agence immobilière victime d'un accès prohibé à son compte de courrier électronique en a informé son assureur, qui a ensuite traité la réclamation déposée contre elle par l'acheteur d'une maison après qu'un cybercriminel a convaincu ce dernier de virer 300 000 $ dollars dans un faux compte bancaire. Les fonds de l'acheteur ont été récupérés, conformément aux modalités de la police de l'agence, et le niveau de protection des comptes de courrier électronique de l'entreprise a été grandement relevé.

- **Fraude par rançongiciel** – Victime d'une attaque par rançongiciel par vol et chiffrement de ses fichiers, l'organisme en a avisé sa compagnie d'assurance qui a fait appel à un enquêteur en criminalistique informatique et à un cabinet d'avocats pour son compte. Ces efforts conjoints ont permis de déjouer l'escroquerie au rançongiciel sans que l'organisme ait à verser de rançon.
- **Fraude par hameçonnage** – Après avoir avisé sa compagnie d'assurance de l'escroquerie par hameçonnage, le coût d'embauche d'un cabinet d'avocats pour contacter les organismes de réglementation et d'une société de service de notification pour informer les personnes concernées et les frais de surveillance du crédit pendant deux ans ont tous été couverts par la police de cyberassurance.
- **Vol d'ordinateur** – La petite entreprise de soins de santé a rapidement informé sa compagnie d'assurance du vol de l'ordinateur portable – contenant le nom, le numéro d'assurance sociale et l'adresse des employés – qui n'a jamais été retrouvé. La compagnie d'assurance a fait appel à un cabinet d'avocats et à une société de criminalistique informatique pour limiter le sinistre de l'assuré et l'aider dans ses efforts de relève.

Sans cyberassurance, les pertes financières et réputationnelles de ces organisations auraient pu être insurmontables.

La probabilité statistique d'une cyberattaque montre tout le sérieux des mesures préventives que devraient prendre les entreprises. Après tout, la survie de votre entreprise peut très bien en dépendre.

**Notes de bas de page**

[1] ALTON, Larry. *How to Protect Your Small Business as Cyber Security Threats Rise*, Small Business Trends, 3 juin 2016, https://smallbiztrends.com/2016/06/cyber-security-strategies.html

[2] Chubb Cyber Index[SM], www.chubbcyberindex.com, mars 2023

[3] *Protecting Your Networks from Ransomware*, www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

## Les auteurs

**Patrick Thielen** est vice-président principal, Risques financiers, chez Chubb et spécialistes des produits d'assurance erreurs et omissions pour les domaines des cyberrisques et de la technologie en Amérique du Nord. Depuis la fusion d'ACE et de Chubb, M. Thielen fait partie des équipes dirigeantes qui ont mis sur pied la division des assurances pour petites entreprises, les polices de gestion du cyberrisque d'entreprise (GCE) et de gestion des risques d'entreprise DigiTech® (GRE DigiTech®), ainsi que le produit Protection contre les cyberrisques Chef-d'œuvre . M. Thielen dirige actuellement les efforts de Chubb pour améliorer et étendre la couverture des cyberrisques et les solutions d'atténuation des risques pour les petites et moyennes entreprises, ainsi que pour les particuliers prospères et leurs familles.

**Dave Charlton** est vice-président directeur de Westchester®, une entreprise de Chubb. À ce titre, il est responsable du développement et de l'offre de produits commerciaux et professionnels spécialisés destinés aux petites et microentreprises de l'Amérique du Nord.

www.chubb.com/ca-fr



Chubb. Insured.[SM]

Mise à jour 02/23