CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

# Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations

Juin 2024

ITSAP.40.001

Les petites et moyennes organisations détiennent de l'information importante qu'elles doivent protéger contre les menaces pour veiller au bon déroulement des activités. Cette information importante comprend entre autres des renseignements sur les clientes et clients et sur les employées et employés, de même que des renseignements commerciaux de nature délicate. Les petites et moyennes organisations sont des cibles probables de cyberattaques puisqu'elles manquent souvent de ressources pour mettre en œuvre des mesures de sécurité. Il se peut que vous ne soyez pas en mesure de protéger toute votre information, mais vous pouvez à tout le moins protéger celle qui est la plus importante pour votre organisation.

## Connaître la valeur de l'information

En connaissant la valeur de l'information de votre organisation, vous pouvez classer par ordre de priorité ce qui doit être protégé. La valeur peut être mesurée sur le plan quantitatif, comme un montant en dollars, et sur le plan qualitatif, comme votre réputation et vos relations avec d'autres entreprises.

Lorsque vous évaluez la valeur de l'information, vous devriez tenir compte des répercussions et du préjudice possible qu'une incapacité de protéger la confidentialité, l'intégrité et la disponibilité des renseignements pourrait occasionner.

- **Confidentialité :** accès non autorisé à de l'information de nature délicate.
- **Intégrité :** modification ou suppression inopportune de l'information.
- **Disponibilité :** perte de l'information ou incapacité d'accéder à l'information.

Lorsque vous déterminez la valeur de l'information, tenez compte des types d'information suivants :

- Information opérationnelle essentielle : information nécessaire au fonctionnement de votre organisation, telle que l'information sur la paie, l'information sur les ventes et les plans d'intervention en cas d'urgence;
- Information de nature délicate : information devant rester confidentielle ou à laquelle seules certaines personnes peuvent accéder, telle que les données personnelles ou financières et la propriété intellectuelle;
- Documents et preuves : information devant être protégée contre toute modification non autorisée, telle que des contrats et des reçus.

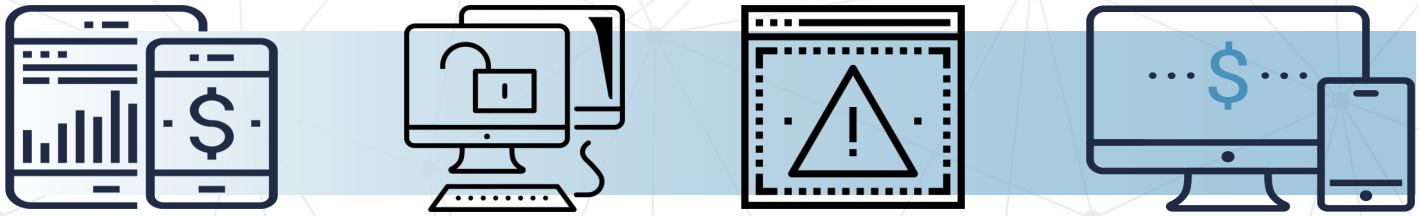
## Établir les menaces et les vulnérabilités

En identifiant les menaces et les vulnérabilités auxquelles fait face votre organisation, vous pouvez mettre en œuvre des mesures de sécurité qui répondent à votre contexte et à vos besoins.
Une menace ou vulnérabilité peut toucher votre organisation d'une façon différente d'une autre organisation, ce qui peut nécessiter l'adoption de mesures de sécurité différentes.

Une **menace** est définie comme étant toute cause possible d'un incident, d'un événement ou d'un acte pouvant nuire à votre organisation ainsi qu'aux systèmes et à l'information organisationnels. Les menaces peuvent être des catastrophes naturelles, comme un incendie et une inondation, ou elles peuvent être d'origine humaine. Réfléchissez aux types de menaces qui pourraient toucher votre organisation en fonction de vos activités et du type d'information que vous détenez.

Une **auteure** ou un **auteur de menace** est la personne qui déclenche une menace, intentionnellement ou non. Les auteures et auteurs de menace peuvent cibler votre organisation pour diverses raisons, notamment pour réaliser un gain financier grâce à l'information volée, pour semer le chaos ou pour se venger.

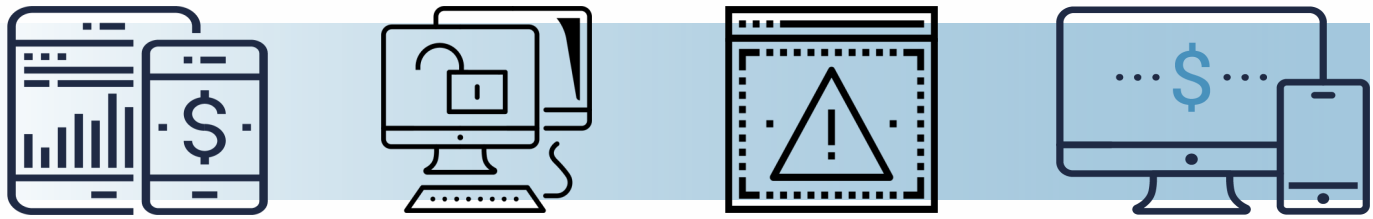
Une **vulnérabilité** est une lacune ou une faiblesse dans vos mesures de sécurité actuelles. Différents facteurs peuvent être à la source des vulnérabilités, comme des versions périmées de logiciels, de l'information non chiffrée, des mots de passe faibles ou des systèmes infectés par un maliciel.



**SÉRIE SENSIBILISATION**



No de cat. D97-1/40-001-2024F-PDF
ISBN 978-0-660-69929-5



## Faire de la cybersécurité une priorité organisationnelle

La cybersécurité devrait faire partie de vos plans et processus opérationnels afin que vous puissiez protéger votre information de grande valeur et votre organisation. Vos clientes et clients s'attendent à ce que vous assuriez la protection de leurs renseignements personnels. De plus, les organisations avec lesquelles vous faites affaire veulent savoir que vous n'exposerez pas leurs systèmes et leur information à des menaces.

Il n'existe pas de solution instantanée ou universelle en sécurité, et le contexte des menaces ne cesse d'évoluer. Pour protéger votre organisation, abordez la sécurité comme un processus continu de prévention, d'établissement et d'élimination des menaces.

Lisez les Contrôles de cybersécurité de base pour les petites et moyennes organisations pour déterminer ceux que vous pouvez mettre en œuvre. Ces contrôles de sécurité peuvent protéger votre organisation et votre information de grande valeur des cybermenaces.

## Pour en savoir plus

Conseils de cybersécurité pour le télétravail (ITSAP.10.116)

Protéger votre organisation contre les maliciels (ITSAP.00.057)

## Protéger l'information de grande valeur

Les réseaux, les systèmes et l'information sécurisés de manière adéquate risquent moins d'être compromis que ceux présentant des lacunes en matière de sécurité. Protégez votre information de grande valeur en appliquant les conseils ci-dessous.

1. Établissement

- Soyez consciente ou conscient de la valeur de votre information.
- Sachez où est stockée l'information de grande valeur.
- Dressez la liste des employées et employés qui ont accès à l'information de grande valeur.
- Sachez comment les employées et employés accèdent à l'information de grande valeur, par exemple à partir d'un lieu de travail à distance.
- Identifiez les vulnérabilités et les menaces.

2. Protection

- Limit Contrôlez l'accès aux systèmes et à l'information de nature délicate.
- Chiffrez les systèmes et l'information de nature délicate.
- Installez les mises à jour logicielles et les correctifs dès qu'ils sont offerts.
- Utilisez des mécanismes de filtrage des courriels et du Web.
- Conservez les appareils ayant accès à l'information de grande valeur dans un endroit sécurisé lorsqu'ils ne sont pas utilisés.
- Avant de procéder à sa disposition, effacez tout le contenu du matériel informatique.

3. Détection

- Utilisez un logiciel antivirus ou antimaliciel.
- Activez, gérez et surveillez les journaux d'activités pour cerner les problèmes ou les incidents.

4. Intervention

- Élaborez un plan d'intervention en cas d'incident.
- Formez les employées et employés sur leurs rôles et responsabilités.

5. Reprise

- Sauvegardez l'information régulièrement.
- Déterminez si une cyberassurance pourrait vous convenir.

6. Examen

- Examinez vos besoins et les systèmes que vous avez en place, et mettez à jour vos systèmes en conséquence pour veiller à ce que l'information de grande valeur demeure protégée.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.