LA CYBER-SÉCURITÉ POUR LES PETITES ET MOYENNES ORGANISATIONS

Ce que vous devez savoir avant de commencer

NORD OUVERT

Mai 2025

TABLE DES MATIÈRES

POURQUOI VOTRE ORGANISATION DEVRAIT-ELLE SE PROTÉGER CONTRE LES MENACES ?

Comprendre les principales menaces : cela peut vous arriver, comme à n'importe quelle autre organisation

Selon la Chambre de commerce du Canada, les petites et moyennes entreprises (PME) sous-estiment souvent les **vulnérabilités en matière de cybersécurité** au sein de leur organisation. En effet, **43 % des cyberattaques ciblent des PME**,[1] Nombre d'entre elles peinent à se relever des cyberattaques qui perturbent leurs opérations et peuvent entraîner des coûts importants.

(1) "A Roadmap to Fortifying the Digital Future of Small Business in Canada"(Hewie, 2023)

En 2023, **59 % des organismes sans but lucratif (OBNL) canadiens ont signalé des fraudes ou des escroqueries** comme l'hameçonnage. L'impact de ces attaques peut être grave, puisque 27 % des OBNL concernées signalent que des incidents de cybersécurité ont empêché l'accès à des ressources ou des services essentiels.[2] Ces vulnérabilités sont préoccupantes car **les OBNL traitent souvent des données personnelles sensibles** et disposent généralement de moins de ressources pour se défendre contre les cybermenaces.

(2) CICP-PCPOB Weekly Report- Rapport Hebdomadaire No. 2.6.20 (CICP-PCPOB, 2024)

Dans ce guide, les petites et moyennes organisations (PMO) font référence à la fois aux PME et aux OBNL.

Les petites et moyennes organisations (PMO) sont de plus en plus exposées aux cyberattaques. Les PMO sous-estiment souvent l'impact que la cybersécurité peut avoir sur leur organisation. Elles manquent de ressources et d'une équipe de sécurité informatique dédiée, et disposent de systèmes obsolètes ou insuffisamment sécurisés pour faire face aux cybermenaces. Ce guide existe pour aider votre PMO à adapter sa stratégie de cybersécurité en fonction des risques et des ressources de votre organisation.

Pas encore convaincu de l'importance de la cybersécurité ?

Consultons quelques statistiques :

- Dans une enquête de 2024,[3] l'Autorité canadienne pour les enregistrements Internet (ACEI) a signalé que 44 % des organisations canadiennes ont été confrontées à une cyberattaque au cours des 12 derniers mois ;
- Dans une évaluation récente, le Centre canadien pour la cybersécurité déclare que le nombre mondial d'incidents de rançongiciel a augmenté de 74 % en 2023 par rapport à 2022, et que la rançon moyenne payée au Canada en 2023 était de 1,13 million de dollars canadiens ;[4]
- En 2023, seulement 14 % des petites organisations à but non lucratif proposaient une formation à la cybersécurité à leur personnel. De plus, seulement 7 % des petites organisations à but non lucratif et 15 % des moyennes organisations déclaraient être conscientes de l'existence de normes de cybersécurité ;[5]
- En 2023, les coûts de récupération suite à des cyberincidents ont doublé depuis 2021,[6] soulignant le besoin croissant de préparation à la cybersécurité au sein des organisations canadiennes ;
- Les menaces en matière de cybersécurité augmentent chaque année, touchant même les grandes organisations publiques canadiennes qui disposent pourtant de davantage de ressources pour se protéger ;[7]
- Malgré la menace accrue, près de la moitié (47 %) des petites entreprises canadiennes interrogées pour le compte du Bureau d'assurance du Canada (BAC)[8] affirment qu'ils n'affectent aucune partie de leur budget de fonctionnement annuel à la cybersécurité ;
- Même si 95 % des cyberattaques sont causées par une erreur humaine,[9] 57 % des petites entreprises au Canada ne proposent toujours pas de formation en matière de cybersécurité ;[10]
- Un récent rapport d'Horizons de politiques Canada[11] souligne les risques en matière de cybersécurité posés par la désinformation générée par l'IA ;
- En 2022, une enquête révélait que 63 %[12] des PME canadiennes ont subi au moins une cyberattaque, ce qui souligne la nature répandue de ces menaces ;
- Cette enquête montre également que 81 % des PME voient l'intelligence artificielle comme un outil qui pourrait renforcer leur cybersécurité mais aussi permettre de nouvelles formes de cyberattaques.

(3) 2024 CIRA Cybersecurity Survey (ACEI, 2024)

(4) Évaluation des cybermenaces nationales 2025-2026 (Centre canadien pour la cybersécurité, 2024)

(5) What Data Tell Us About Cybersecurity in Canadian Nonprofits (Shim and Barr, 2024)

(6) L'incidence du cybercrime sur les entreprises canadiennes (Statistique Canada, 2024)

(7) As We Enter 2024, Cyberthreats to Canada Are Growing (Hilt, 2023)

(8) Many small businesses vulnerable to cyber attacks (IBC, 2021)

(9) The Global Risks Report 2022 (Forum économique mondial)

(10) Cyber Attacks: Not a matter of if, but when - and what's next? (Mastercard)

(11) Perturbations à l'horizon (Horizons de politiques Canada, 2024)

(12) Cybercrime strikes more than six in 10 Quebec companies (KPMG, 2023)

Qu'est-ce que la cybersécurité ? La triade CIA et son rôle dans la protection de votre organisation

Le terme **cybersécurité** peut être défini comme « toute technologie, mesure ou pratique visant à prévenir les cyberattaques ou à atténuer leur impact ».[13] Ses principaux objectifs sont de **protéger les composantes de la triade CIA, qui signifie Confidentialité, Intégrité et Disponibilité (*Availability*).**[14]

Lorsque ces trois composantes sont correctement prises en compte par une organisation, celle-ci est mieux à même d'atténuer les menaces liées à la cybersécurité. Chaque composante est définie comme suit :

(13) What is Cybersecurity (Lindemulder, Kosinski, 2024)

(14) What is the CIA Triad? (Fortinet)

TERME	DÉFINITION
Confidentialité	**Protéger la confidentialité des informations au sein d'une organisation** Garantir que les informations commerciales sensibles ne sont accessibles qu'aux personnes autorisées. LA confidentialité permet la protection des secrets de votre organisation grâce aux éléments suivants : ▪ Contrôle des accès (les bonnes personnes accèdent aux bonnes informations) ▪ Cryptage des données ▪ Politiques claires en matière d'utilisation des appareils personnels ▪ Formation régulière de sensibilisation à la cybersécurité
Intégrité	**Garantir l'intégrité des données en s'assurant que les informations utilisées sont authentiques, exactes, fiables et qu'elles n'ont pas été altérées.** L'intégrité garantit l'exactitude et la fiabilité des données de votre organisation grâce aux éléments suivants : ▪ Protection contre les modifications non autorisées ▪ Audits réguliers des données pour en vérifier l'authenticité ▪ Vérification régulière de l'exactitude des données ▪ Procédures de sauvegarde systématique avec contrôles d'intégrité
Disponibilité (*Availability*)	**Veiller à ce que les systèmes et les données soient accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin** La mise à disposition des données aux utilisateurs autorisés nécessite les éléments suivants : ▪ Mises à jour et maintenance régulières du système ▪ Stratégie de sauvegarde complète (sur site et hors site) ▪ Protection contre les interruptions de service ▪ Mesures de protection contre les rançongiciels

Il est essentiel de comprendre ces principes fondamentaux de la cybersécurité - Confidentialité, Intégrité et Disponibilité - car **ils sont à la base des exigences légales et des normes de conformité**. Examinons maintenant les obligations légales spécifiques au Canada qui pourraient s'appliquer à votre organisation et comment celles-ci sont liées à la protection de vos données et de vos systèmes.

La cybersécurité est-elle une exigence légale pour mon organisation ?

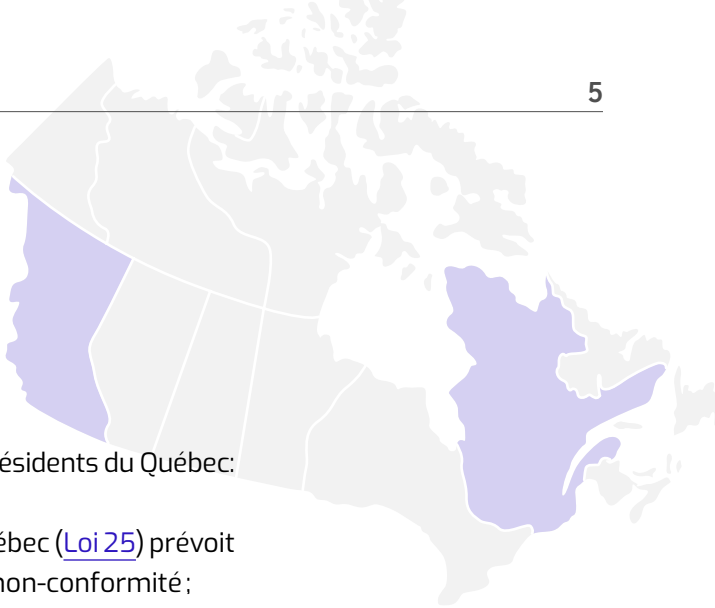
Si votre organisation recueille, utilise ou divulgue des renseignements personnels au Canada, vous avez l'obligation légale de les protéger. **La confidentialité des données et la cybersécurité vont de pair**. Le non-respect de ces obligations peut entraîner des sanctions sévères, des pertes financières et des atteintes à la réputation.

Principales lois canadiennes sur la protection de la vie privée

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) est la principale loi fédérale sur la protection de la vie privée qui oblige les organisations à :

- Protéger les renseignements personnels grâce à des mesures de sécurité appropriées ;
- Obtenir le consentement avant de collecter, d'utiliser ou de divulguer des renseignements à caractère personnel ;
- Signaler les failles de sécurité importantes en matière de données aux personnes et aux autorités concernées ;[15]
- Les organisations peuvent faire face à des amendes allant jusqu'à 100 000 $ en cas d'infraction à la LPRPDE.

(15) Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité (Commissariat à la protection de la vie privée du Canada)



Si votre organisation se trouve au **Québec** ou traite des données de résidents du Québec:

- La Loi sur la protection des renseignements personnels du Québec (Loi 25) prévoit des amendes allant jusqu'à 10 millions de dollars en cas de non-conformité ;
- Elle exige un consentement explicite pour toutes les technologies de traçage ;
- Elle rend obligatoires la nomination d'un responsable de la protection de la vie privée et la réalisation d'évaluations des facteurs relatifs à la vie privée.

Si votre organisation se trouve en **Colombie-Britannique** (BC) ou traite des données de résidents de la Colombie-Britannique :

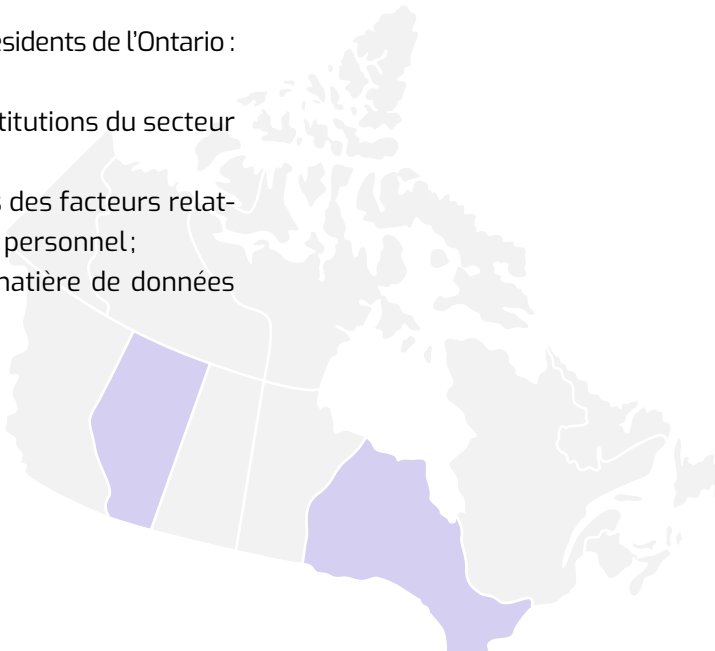
- La Loi sur la protection des renseignements personnels de la Colombie-Britannique (PIPA) prévoit des amendes allant jusqu'à 100 000 $;
- Elle s'applique à toute organisation privée collectant des renseignements personnels sur des résidents de la Colombie-Britannique ;
- Elle exige des organisations qu'elles protègent les renseignements personnels contre toute utilisation non autorisée.

Si votre organisation se trouve en **Alberta** ou traite des données de résidents de l'Alberta :

- La loi PIPA de l'Alberta prévoit des amendes allant jusqu'à 100 000 $;
- Elle règlemente toutes les organisations du secteur privé qui traitent les données des résidents de l'Alberta ;
- Elle impose un objectif raisonnable et une collecte limitée des renseignements à caractère personnel.

Si votre organisation est située en **Ontario** ou traite des données de résidents de l'Ontario :

- Les récentes modifications à la loi FIPPA s'appliquent aux institutions du secteur public provincial de l'Ontario ;
- Celles-ci sont dans l'obligation de procéder à des évaluations des facteurs relatifs à la vie privée avant de collecter des données à caractère personnel ;
- Elles ont l'obligation de signaler les failles de sécurité en matière de données lorsqu'il existe un risque réel significatif.



Règlementations supplémentaires

Votre organisation devra peut-être également se conformer aux textes suivants :

- LCAP – Loi canadienne anti-pourriel
  - S'applique aux organisations envoyant des messages électroniques commerciaux.
  - Les amendes peuvent aller jusqu'à 10 millions de dollars pour les organisations et 1 million de dollars pour les particuliers.
- Autres lois provinciales sur l'informations en matière de santé comportant des exigences de confidentialité et des amendes importantes
  - Loi sur les renseignements de santé et de services sociaux du Québec (Projet de loi 3)
  - Loi sur la protection des renseignements personnels sur la santé de l'Ontario (PHIPA)
  - Loi sur l'accès et la protection en matière de renseignements personnels sur la santé du Nouveau-Brunswick
  - Loi visant à assurer la protection des renseignements personnels sur la santé de Terre-Neuve-et-Labrador
  - Loi sur les renseignements personnels sur la santé de la Nouvelle-Écosse

Comment protéger votre organisation

Pour garantir la conformité légale, pensez à :

- Nommer un responsable de la protection de la vie privée issu d'une formation juridique, informatique ou opérationnelle ;
- Mettre en œuvre d'un audit complet de conformité juridique en matière de protection de la vie privée et de cybersécurité ;
- Former le personnel à la gestion des risques en matière de protection de la vie privée et de cybersécurité.

Votre organisation exerce-t-elle ses activités au Québec ? Consultez le Guide de Nord Ouvert sur la conformité en matière de protection de la vie privée au Québec !

QUE PEUT FAIRE MON ORGANISATION POUR SE PROTÉGER CONTRE LES MENACES LIÉES À LA CYBERSÉCURITÉ ?

Ce que vous pouvez faire dès maintenant, sans aide extérieure

Souvent négligées dans les cadres conçus pour les grandes entreprises du secteur public et privé, les organisations à but non lucratif sont confrontées à des défis uniques, notamment le manque de personnel formé à la cybersécurité et le manque de budget. Selon un rapport récent, **68 % des organisations à but non lucratif n'ont pas mis en place de politiques et de procédures en matière de cybersécurité et n'ont pas de plan d'intervention en cas de cyberattaque.**[16] Cette expertise limitée en matière de cybersécurité et le manque de connaissances spécifiques les rendent susceptibles de devenir des cibles privilégiées pour les cyberattaquants. Pour les PMO, le développement d'une culture et d'une sensibilisation à la sécurité et la mise en œuvre d'une formation adéquate peuvent contribuer à détecter et à prévenir les cyberattaques.

(16) "Cybersecurity Challenges and Best Practices for Nonprofits" (Eide Bailly)

La mise en œuvre des meilleures pratiques en matière de cybersécurité est complexe. **Cette liste de contrôle permet une première auto-évaluation des principaux risques en matière de cybersécurité et met en lumière les meilleures pratiques pour les atténuer.** La réalisation de l'auto-évaluation peut aider les organisations à trouver des conseils supplémentaires pour améliorer leur posture de sécurité, tout en prenant en compte les spécificités de leur équipe informatique.

Sensibilisation et formation organisationnelle

- L'organisation dispense-t-elle aux employés une formation actualisée sur la lutte contre l'hameçonnage et l'ingénierie sociale, et a-t-elle mis en place des politiques et des procédures en cas d'attaques de ce type ?
- L'organisation fournit-elle des conseils et des recommandations sur les politiques relatives aux mots de passe et sur l'accès aux services, aux logiciels et au matériel en nuage ?
- L'organisation propose-t-elle une formation d'intégration aux nouveaux employés et une formation annuelle sur la reconnaissance et la prévention des attaques par hameçonnage ?
- L'organisation forme-t-elle son personnel à la manière de signaler efficacement les cyberattaques et les attaques par hameçonnage suspectées ou confirmées ?
- L'organisation assure-t-elle une sensibilisation permanente aux politiques et procédures existantes afin de s'assurer que le personnel sait ce que l'on attend de lui ?

Inventaire du matériel et des logiciels

- L'organisation dispose-t-elle d'un registre détaillé des actifs matériels et logiciels et de procédures permettant de s'assurer qu'il est à jour ?
- L'organisation tient-elle un inventaire complet de ses données et des points d'accès correspondants afin de faciliter la mise en œuvre efficace des restrictions d'accès au système ?
- L'organisation dispose-t-elle de politiques et de procédures en matière d'acquisition et d'installation de nouveaux logiciels ?
- L'organisation dispose-t-elle d'une liste de contrôle concernant la restitution des actifs technologiques détenus par les employés, y compris les contrôles d'accès, les changements de mot de passe, la restitution du matériel et les procédures d'effacement ?
- L'organisation alloue-t-elle un budget annuel pour les mises à jour technologiques ?
- L'organisation dispose-t-elle de procédures pour évaluer ses actifs technologiques ?

Gestion des données

- L'organisation dispose-t-elle de politiques de gouvernance des données couvrant la collecte, la conservation et l'élimination des données ?
- L'organisation a-t-elle mis en place des politiques, des procédures et des protocoles de sauvegarde des données afin de prévenir la perte de données et de permettre une récupération rapide ?
- L'organisation veille-t-elle à ce que le consentement à l'utilisation des données dans le cadre d'activités de recherche soit clairement communiqué et normalisé d'un projet à l'autre, en particulier pour les données qui pourraient être utilisées à des fins autres que la recherche ?
- Des mesures de contrôle d'accès aux informations sensibles sont-elles mises en place au sein de l'organisation ? Dans l'affirmative, ces contrôles d'accès font-ils l'objet d'une surveillance et d'un examen, et à quelle fréquence ?

Moyens et pratiques de sécurité

- L'organisation dispose-t-elle d'une équipe interne ou d'une assistance informatique externe ?
- Si l'organisation a des employés qui travaillent à domicile, dispose-t-elle d'une politique de télétravail conforme aux meilleures pratiques en matière de cybersécurité ?
- L'organisation dispose-t-elle de politiques et de procédures de sécurité pour les appareils personnels (téléphones, tablettes ou ordinateurs personnels) lorsque les employés les utilisent pour accéder à la messagerie professionnelle, aux services en ligne ou à d'autres systèmes de l'organisation ?
- L'organisation chiffre-t-elle les dispositifs internes à l'organisation, tels que les ordinateurs portables ?
- L'organisation s'assure-t-elle que le personnel utilise des connexions VPN sécurisées lorsqu'il travaille en dehors du bureau ? Cette procédure est-elle en place à la fois pour les nouveaux employés et les employés actuels ?
- L'organisation automatise-t-elle les mises à jour des défenses de sécurité pour le matériel ?
- L'organisation utilise-t-elle des services en nuage et, dans l'affirmative, les ordinateurs portables sont-ils configurés pour envoyer automatiquement les fichiers de travail vers le nuage ?
- L'organisation dispose-t-elle d'un gestionnaire de mots de passe pour sécuriser les comptes utilisés dans l'ensemble de l'organisation ?
- L'organisation exige-t-elle une authentification à deux facteurs (2FA) sur les appareils mobiles ainsi que des gestionnaires de mots de passe pour réduire le risque d'accès non autorisé ?

Conformité juridique

- L'organisation attribue-t-elle des responsabilités et des obligations en matière de conformité à ses dirigeants actuels (qui comprennent aussi bien la direction que le conseil d'administration) ? On entend par « responsables de la conformité » les personnes qui prennent des décisions sur la manière dont l'organisation doit se conformer à des exigences déterminées.
- L'organisation examine-t-elle régulièrement la législation relative au respect de la vie privée afin de s'assurer qu'elle suit les lignes directrices et les meilleures pratiques établies par les autorités compétentes, même si cela n'est pas nécessairement requis par la loi ?
- Votre organisation dispose-t-elle de politiques, de procédures et d'une gestion des tiers en matière de respect de la vie privée ?

Gestion des fournisseurs

- L'organisation examine-t-elle les accords actuels et futurs avec des fournisseurs de technologies tiers pour s'assurer qu'ils sont conformes aux politiques internes ?
- L'organisation veille-t-elle à ce que les fournisseurs de sites web et de services de marketing externes imposent des restrictions d'accès aux hébergeurs de sites web afin que les adresses électroniques ne puissent pas être contrôlées ou partagées par les services de marketing ?
- L'organisation exige-t-elle des fournisseurs de services de sécurité qu'ils l'informent des changements importants ? Par exemple, si votre fournisseur de VPN est racheté par une autre société susceptible d'avoir des politiques différentes en matière de protection de la vie privée et de sécurité.

Capacité de réaction en cas de violation de données

- L'organisation dispose-t-elle d'un plan complet d'intervention en cas de violation de la cybersécurité qui soit facilement accessible au personnel clé ?
- L'organisation dispose-t-elle d'un plan de communication de crise en cas d'infraction ou de cyberattaque ?

Maintenant que votre organisation a identifié les problèmes de cybersécurité, vous pouvez passer à l'action.

L'utilisation de cette liste de contrôle peut aider votre organisation à comprendre ses forces et faiblesses actuelles en matière de cybersécurité sans avoir recours à une expertise externe. Toutefois, la cybersécurité est un processus continu plutôt qu'un exercice ponctuel. S'il est important de connaître l'existence des plans et des politiques en place, il est tout aussi nécessaire de s'assurer qu'ils sont adéquats, compris et mis en œuvre par le personnel. Certains problèmes identifiés peuvent être résolus en interne tandis que d'autres peuvent nécessiter des conseils externes pour mettre en œuvre des solutions.

Ce qu'il faut envisager pour aller plus loin : l'importance des audits et des évaluations de la cybersécurité

Après avoir effectué l'auto-évaluation proposée précédemment, un audit de cybersécurité ou une évaluation menée par des experts externes peuvent s'avérer cruciaux pour identifier et traiter les vulnérabilités en matière de sécurité. Si ces deux approches contribuent à l'amélioration des pratiques de sécurité, elles répondent à des objectifs différents. Un audit externe fournit une vérification indépendante et détaillée de vos mesures de sécurité par rapport à des normes spécifiques, qui peuvent être définies par les politiques de votre organisation, les meilleures pratiques de l'industrie ou les exigences légales. Une évaluation offre une vision plus large de votre sécurité, de votre santé et de vos risques. Les petites et moyennes organisations doivent choisir en fonction de leurs besoins spécifiques : si vous avez besoin d'un examen complet et indépendant de votre conformité en matière de sécurité, un audit externe est plus approprié. Si vous voulez comprendre et améliorer votre position globale en matière de sécurité avec plus de souplesse, une évaluation peut être le meilleur choix. Les organisations peuvent toujours commencer par une évaluation de la cybersécurité et décider en connaissance de cause si un audit est une étape nécessaire et bénéfique. Si votre organisation choisit de procéder à un audit, il est recommandé de mettre en place un processus d'évaluation préalable à l'aide d'une matrice des risques, et ce, que l'audit soit réalisé avec des ressources internes ou externes.

ASPECT	AUDIT DE CYBERSÉCURITÉ	ÉVALUATION DE LA CYBERSÉCURITÉ
Objectif	Vérifier le respect de normes de sécurité spécifiques et évaluer l'efficacité des contrôles existants.	Fournir une analyse de haut niveau de l'état général de la sécurité et identifier les faiblesses.
Description	Un examen détaillé des contrôles de sécurité, des politiques et des procédures par rapport aux exigences spécifiques du cadre (par exemple, LPRPDE, loi 25, etc.).	Une évaluation générale de la maturité de la sécurité et de l'efficacité des contrôles, en mettant l'accent sur l'identification des vulnérabilités et des risques.
Résultats	Un aperçu de la conformité et un rapport détaillé sur les lacunes en matière de contrôles de sécurité, ainsi que des recommandations spécifiques pour respecter les normes.	Des informations sur les risques de sécurité, les vulnérabilités classées par ordre de priorité et des recommandations pour améliorer les pratiques générales en matière de cybersécurité.

Comment se préparer à un audit de cybersécurité : vos documents d'évaluation sont-ils en ordre ?

Un audit de cybersécurité est une étape cruciale dans l'identification et la résolution des failles de sécurité qui mettent en péril les données et les opérations de votre organisation. Pour que l'audit soit efficace et utile, votre organisation doit préparer correctement la documentation. La **liste de contrôle d'auto-évaluation de l'état de préparation à l'audit** aide les organisations à identifier les éléments essentiels à mettre en place avant de faire appel à des auditeurs externes.

En remplissant cette liste de contrôle, votre organisation pourra identifier les lacunes dans sa documentation, ses processus et ses contrôles qu'il convient de combler en priorité. Cette préparation sert de **feuille de route pour rendre le processus d'audit plus efficace** en rassemblant la documentation nécessaire et en préparant le personnel au processus d'audit, l'organisation s'assurera ainsi que ce dernier fournira des informations significatives sur les risques de sécurité réels.

Gestion des actifs et de la documentation

- L'organisation tient-elle à jour un inventaire de tous les ordinateurs, équipements, licences de logiciels et lieux de stockage de données ?
- L'organisation tient-elle à disposition des procédures de sécurité écrites et les met-elle régulièrement à jour pour consultation ?
- L'organisation a-t-elle identifié les données, les logiciels et les biens physiques qui lui sont indispensables ? Il peut s'agir par exemple de données financières ou de données relatives aux clients, d'applications essentielles et de serveurs de données.

Cadre politique

- L'organisation a-t-elle documenté sa tolérance au risque de sécurité, en définissant le niveau de risque qu'elle est prête à accepter ?
- L'organisation a-t-elle identifié les meilleures pratiques et normes en matière de création de politiques de cybersécurité ? (par exemple ITSAP.00.137 - Centre canadien de cybersécurité, ISO 27001 et 27002, ou NIST CSF)
- Existe-t-il une procédure écrite pour l'octroi et le retrait de l'accès au système lorsque des membres du personnel rejoignent ou quittent l'organisation ?

Infrastructure

- L'organisation fournit-elle des conseils et des recommandations sur les politiques de mot de passe, l'accès aux services en nuage, les logiciels et le matériel ?
- L'organisation utilise-t-elle des services en nuage et, si oui, les ordinateurs portables sont-ils configurés pour envoyer automatiquement les fichiers de travail vers le nuage ?

Préparation de l'équipe

- L'équipe informatique dispose-t-elle de cartographies actualisées de la configuration du réseau ?
- Existe-t-il une liste des utilisateurs privilégiés et des administrateurs système ?

Réponse en cas d'incident

- Existe-t-il un plan par étapes pour gérer les incidents de cybersécurité ?
- Les événements et incidents liés à la sécurité sont-ils systématiquement enregistrés ?

Gestion des risques

- L'organisation a-t-elle procédé à un examen de base afin d'identifier les points faibles en matière de cybersécurité ?
- L'organisation tient-elle à jour une liste des problèmes de sécurité connus et prévoit-elle de les résoudre ?

Respect de la vie privée

- L'organisation a-t-elle identifié les lois relatives à la protection de la vie privée qui s'appliquent à ses activités ?
- L'organisation tient-elle des registres pour montrer de quelle manière elle se conforme à ces lois ?

Formation et documentation

- Existe-t-il des documents relatifs aux sessions de formation du personnel en matière de cybersécurité ?
- Une formation spécialisée en matière de sécurité est-elle documentée pour le personnel technique (informatique, RH, financier) ?

Maintenant que vous avez évalué votre sécurité interne à l'aide de la liste de contrôle ci-dessus, il est essentiel de **ne pas se limiter aux frontières limites de votre organisation**. Vos activités dépendent probablement de divers fournisseurs de services externes - du stockage en nuage aux services de messagerie - qui peuvent présenter des risques de sécurité supplémentaires pour votre organisation. Voyons comment faire en sorte que ces partenaires respectent le même niveau d'engagement en matière de sécurité que celui que vous vous efforcez d'atteindre.

Garantie de sécurité tierce : vos données sont-elles en sécurité chez vos fournisseurs de services ?

Dès nos jours, les organisations font de plus en plus appel à des fournisseurs de services externes pour leurs opérations essentielles, qu'il s'agisse du stockage de données dans le nuage ou de la gestion des courriels et des informations sur les clients. Bien que ces services soient nécessaires pour la plupart des organisations, ils peuvent créer des risques de sécurité. Un incident de sécurité chez un fournisseur de services peut avoir un impact direct sur la sécurité de votre organisation.

Pourquoi se préoccuper de la sécurité des fournisseurs de services ?

- Les données et les opérations de votre organisation dépendent de ces fournisseurs
- Vous êtes responsable de la protection de vos données, même lorsqu'elles sont entre les mains de quelqu'un d'autre.

Qu'est-ce qu'un rapport d'assurance raisonnable de la sécurité

Les fournisseurs de services tels que Microsoft, Amazon ou votre société informatique locale doivent être en mesure de prouver leurs mesures de sécurité par le biais d'évaluations indépendantes de sécurité. Ces évaluations donnent lieu à des rapports standardisés que vous pouvez réclamer et examiner :

- Rapports SOC 2 : une norme internationalement reconnue pour les contrôles de sécurité
- NCMC 3000 : une norme canadienne qui évalue les mesures de sécurité

Ces rapports vérifient cinq domaines clés qui sont essentiels à votre organisation : la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la protection de la vie privée.

Conseils pratiques pour votre organisation

- Lorsque vous choisissez de nouveaux fournisseurs de services, demandez-leur s'ils ont des rapports SOC 2 ou NCMC 3000 ;
- Intégrez l'exigence de ces rapports d'assurance en matière de sécurité dans vos contrats de service ;
- Examinez ces rapports chaque année ou lors du renouvellement des contrats ;
- N'oubliez pas que les fournisseurs peuvent facturer un supplément pour ces rapports en raison de leur coût.

Attention : Votre organisation ne peut pas contrôler ou inspecter directement les grands fournisseurs de services tels que Microsoft ou Amazon. C'est pourquoi ces **rapports de sécurité indépendants sont essentiels** : ils vous donnent l'assurance que vos fournisseurs maintiennent des mesures de sécurité appropriées.

COMMENCEZ DÈS AUJOURD'HUI !

Il est maintenant temps de mettre en œuvre les mesures de cybersécurité dans votre organisation. Voici quelques **ressources supplémentaires qui peuvent vous aider** dans votre processus d'évaluation et de mise en œuvre.

Encore plus de listes de contrôle

Explorez, utilisez et adaptez d'autres listes de contrôle de Nord Ouvert en matière de cybersécurité :

- Liste de contrôle - Meilleures pratiques en matière de cybersécurité pour les PMO
- Auto-évaluation de la protection de la vie privée : La protection des renseignements personnels au Québec (Loi 25)
- Auto-évaluation de la protection de la vie privée : LPRPDE et PIPA (Colombie-Britannique et Alberta)

Évaluation de la maturité

Nos évaluations de maturité fournissent une vue approfondie des capacités de votre organisation en matière de données et de son état de préparation à une transformation plus poussée. Ces évaluations s'appuient sur des normes et des critères de référence du domaine pour mesurer les performances et mettre en évidence les domaines à améliorer :

- **Évaluation de la maturité des données** : Nous évaluons la manière dont votre organisation gère ses données, de la collecte et du stockage à la gestion de la qualité et à la gouvernance, en fournissant une feuille de route pour améliorer vos capacités en matière de données.
- **Évaluation de la conformité en matière de protection de la vie privée** : Nous procédons à une évaluation complète des risques en matière de protection de la vie privée et fournissons des recommandations pour améliorer la conformité de votre organisation avec les règlementations pertinentes en matière de protection de la vie privée.
- **Évaluation de la cybersécurité** : Nous évaluons vos défenses en matière de cybersécurité, vous aidant à identifier les vulnérabilités et à mettre en place une défense plus solide contre les cybermenaces.

À Propos de Nord Ouvert

Nord Ouvert est une organisation à but non lucratif qui se consacre à l'avancement du bien commun. En collaboration avec des gouvernements et des organisations civiques de toutes tailles, nous fournissons une expertise en matière de données afin d'améliorer la prise de décision, de stimuler l'innovation, d'optimiser les services publics et civiques et de relever les défis les plus urgents de la société. Notre travail couvre l'ensemble du cycle de vie des données, avec un accent particulier sur la gouvernance des données - en guidant les décisions humaines qui déterminent si les données sont utiles, exploitables, sécurisées et dignes de confiance.

Auteurs: Cristiano Therrien, Jérémy Diaz, Judith François-Langevin, Tona Mutimura, Merlin Chatwin, Christian Medina, John Griffin

Ce travail est protégé par le droit d'auteur de Nord Ouvert sous licence Creative Commons 4.0 International (CC BY 4.0), à l'exception des photographies, des images, des logos, de la marque et des autres marques de commerce de Nord Ouvert.

Contactez Nord Ouvert (info@opennorth.ca) pour savoir comment nous pouvons aider votre organisation

Canada Montréal DÉFI DES VILLES INTELLIGENTES Montréal en commun

La cybersécurité pour les petites et moyennes organisations