Vérificateur général
MANITOBA

Rapport à l'Assemblée législative du Manitoba

Réponse aux incidents de cybersécurité à Soins communs

Rapport d'assurance indépendant

VERSION DU SITE WEB

Décembre 2024

Cette page a été laissée
blanche intentionnellement.

La traduction de ce rapport a été fournie par le Service de traduction du Manitoba. En cas d'incohérence, se reporter à la version anglaise.

VERSION DU SITE WEB

Cette page a été laissée
blanche intentionnellement.

Table des matières

Cette page a été laissée
blanche intentionnellement.

Commentaires du vérificateur général

Les systèmes d'information du secteur public sont essentiels pour la prestation de services aux Manitobains. Ces systèmes contiennent une multitude de données, y compris des renseignements personnels et d'autres informations sensibles. En raison de la criticité des services et de la nature de ces données, ces systèmes sont de plus en plus exposés aux cyberattaques, notamment aux rançongiciels et au vol de données.

Au cours des dernières années, nous avons publié plusieurs rapports d'audits informatiques qui ont mentionné la nécessité d'améliorer les contrôles de cybersécurité dans l'ensemble du secteur public. L'amélioration de ces contrôles réduit le risque que des acteurs malveillants puissent accéder à ces systèmes d'information. Cependant, même avec les contrôles les plus robustes en place, des cyberattaques restent possibles. Les organismes du secteur public doivent être prêts à réagir en cas d'incidents de cybersécurité afin de minimiser l'impact sur leurs activités et la perte potentielle de données.

Dans le cadre de cet audit, nous avons examiné l'état de préparation de Soins communs en matière de réponse aux incidents de cybersécurité. Il reste cependant du travail à faire. Soins communs doit effectuer des exercices pour tester son plan de réponse aux incidents de cybersécurité, améliorer la formation et compléter son plan de communication externe.

Ce rapport comprend quatre recommandations qui aideront Soins communs à mieux se préparer à répondre à une attaque de cybersécurité. Bien que ces recommandations s'adressent spécifiquement à Soins communs, tous les organismes du secteur public doivent prendre des mesures pour être prêts à répondre aux incidents de cybersécurité.

Je tiens à remercier la direction et le personnel de Soins communs pour leur coopération et leur assistance tout au long de l'audit, et j'exprime ma gratitude à mon équipe d'audit pour les efforts qu'elle a déployés afin de mener à bien ce travail important.

Original signé par :
Tyson Shtykalo, FCPA, FCA
Vérificateur général

Audits récents où les faiblesses dans les contrôles de cybersécurité ont été abordées :

- *Gestion de la sécurité des TI en lien avec l'accès à distance* (2024)
- *Accès privilégiés aux systèmes d'information* (2022)
- *Vieillissement des systèmes d'information* (2022)
- *Bureau de l'état civil* (2020)
- *DossiÉ Manitoba* (2018)

Cette page a été laissée
blanche intentionnellement.

Points saillants du rapport

Motifs de l'audit

- Des systèmes d'information fiables et accessibles sont essentiels à la fourniture de services de santé publics.
- Ces systèmes sont susceptibles de faire l'objet de cyberattaques en raison de la criticité des services qu'ils soutiennent et de la multitude de renseignements personnels qu'ils contiennent.
- Nous avons voulu déterminer si Soins communs disposait d'un processus permettant de répondre rapidement aux incidents de cybersécurité, ce qui en minimiserait l'impact sur les opérations de santé et la perte de données.

Conclusion

Soins communs dispose d'un processus permettant de répondre rapidement aux incidents de cybersécurité, mais les tests réguliers et la formation peuvent être améliorés.

Le présent rapport d'audit comprend 4 RECOMMANDATIONS.

Nos constatations

Plan de réponse aux incidents de cybersécurité (RICS)

Soins communs dispose d'un plan permettant de répondre aux incidents de cybersécurité, mais une meilleure formation est nécessaire et certaines pratiques à l'appui du plan doivent être documentées.

- Une norme de sécurité, un plan et des procédures à l'appui ont été élaborés, et le personnel de Soins communs ainsi que des ressources externes sont prêts à répondre aux incidents de cybersécurité.
- Tous les membres de l'équipe responsable de la RICS, qui est chargée de répondre aux incidents de cybersécurité et de les gérer, n'ont pas bénéficié de séances de formation.
- Aucun plan de communication avec les intervenants externes en cas d'attaque de cybersécurité n'est en place, et les procédures relatives aux incidents de rançongiciel et d'extorsion sont encore en cours d'élaboration.

Mise à l'essai du plan

Aucun exercice n'est effectué pour mettre à l'essai le plan de RICS

- Il faut mettre à l'essai les plans afin de s'assurer d'être prêts à réagir aux incidents de cybersécurité.

Mise en œuvre du plan

Des processus sont en place pour déclencher le plan de RICS en cas de besoin.

- La détection et l'analyse des incidents de cybersécurité sont couvertes par le processus de gestion des incidents de Soins communs.

Cette page a été laissée
blanche intentionnellement.

Contexte

Le système de soins de santé de la Province du Manitoba (la Province) est assuré par divers organismes, notamment :

- Santé Manitoba.
- des organismes de prestation de services.
  - Soins communs
  - cinq offices régionaux de la santé (y compris les organismes contrôlés par ces offices) :
    - Office régional de la santé d'Entre-les-Lacs et de l'Est
    - Office régional de la santé du Nord
    - Santé de Prairie Mountain
    - Southern Health–Santé Sud
    - Office régional de la santé de Winnipeg
  - Action cancer Manitoba.

Santé Manitoba est le ministère du gouvernement du Manitoba qui oriente la planification et la prestation des services de santé dans toute la province. Le fonctionnement de ce ministère est régi par des dispositions législatives et relève des responsabilités de la ministre de la Santé.

Soins communs, créé en 2018, est l'office provincial de la santé. Il fournit des services à l'échelle de la province afin de rationaliser la prestation des soins de santé et de réduire la duplication des services de soutien, y compris la gestion des technologies de l'information et de la communication pour les organismes de prestation de services. Cela permet à ces organismes de se concentrer sur la prestation de services de santé. Soins communs utilise un modèle de services partagés pour réduire la complexité et renforcer l'efficience du système de soins de santé dans la province. Les Services numériques partagés font partie de ce modèle de services partagés, fournissant des services technologiques à Soins communs et aux autres organismes de prestation de services. Ses fonctions comprennent la gestion du programme de cybersécurité.

Les Services numériques partagés disposent d'une norme de réponse aux **incidents de cybersécurité** (la norme de RICS) qui décrit les exigences, les normes et les spécifications de base en matière de sécurité afin de se préparer à fournir une réponse efficace à un incident de sécurité de l'information. Cette norme définit les exigences essentielles en matière de contrôle administratif et technique de sorte que les Services numériques partagés puissent détecter et gérer les incidents de cybersécurité et y répondre de manière à en minimiser l'impact ou le préjudice sur les actifs informatiques, la prestation des services de santé et les besoins des patients.

Un **incident de cybersécurité** est un événement qui compromet dans les faits ou de manière imminente, sans autorisation légale, l'intégrité, la confidentialité ou la disponibilité de renseignements ou d'un système d'information.

Source : Plan de réponse aux incidents de cybersécurité de Soins communs

Le plan de réponse aux incidents de cybersécurité (le plan de RICS) soutient la norme de RICS en fournissant des orientations pour la gestion des activités lors d'incidents de cybersécurité de priorité élevée ou critique. Son objectif est d'assurer une réponse cohérente et efficace pour limiter et minimiser l'impact possible de ces incidents. Le plan de RICS fournit des conseils sur les points suivants :

- La définition du terme « incident de cybersécurité » et la classification des incidents par ordre de priorité.
- Les rôles et responsabilités nécessaires pour gérer efficacement les événements de cybersécurité, y compris la définition de l'équipe responsable de la RICS.
- Le processus de réponse et de gestion efficace des incidents de cybersécurité.

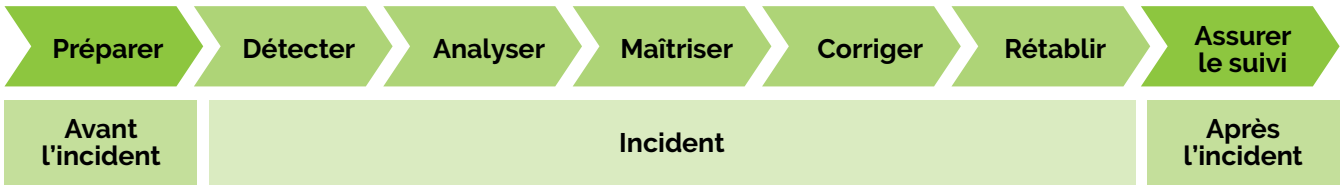
Un pare-feu est un dispositif sur lequel est installée une application de protection du réseau afin de protéger le réseau contre les intrusions intentionnelles ou involontaires. Un pare-feu se situe au point de jonction ou à la passerelle entre deux réseaux, généralement un réseau privé et un réseau public tel qu'Internet.

Source : NIST SP 800-35

Le plan de RICS fait la distinction entre un événement et un incident de sécurité, ce qui permet de prendre les mesures appropriées en fonction de la gravité et de l'impact potentiel. Un événement est un phénomène observable dans un système ou un réseau. Il s'agit par exemple de l'envoi d'un courriel par un utilisateur ou du blocage d'une tentative de connexion par **un pare feu**. Un incident de sécurité est un événement qui compromet dans les faits ou de manière imminente, sans autorisation légale, l'intégrité, la confidentialité ou la disponibilité de renseignements ou d'un système d'information.

Le plan de RICS décrit le processus en sept étapes suivi par Soins communs pour gérer les incidents de cybersécurité. Ces étapes sont les suivantes :

Figure 1 : Processus de réponse aux incidents de cybersécurité à Soins communs



Le plan de RICS est déclenché lorsqu'un événement a été classé comme incident de cybersécurité de priorité élevée ou critique. La classification initiale de l'événement se fait au cours du processus général de gestion des incidents de Soins communs, où tous les événements sont enregistrés dans l'outil de gestion des services de technologie de l'information (GSTI) de l'organisme. Ces événements sont enregistrés par le bureau d'assistance et peuvent avoir pour origine les utilisateurs de Soins communs

ou son **fournisseur de services de sécurité gérés** (FSSG). Le FSSG sert de **centre des opérations de sécurité** et est à ce titre responsable de la surveillance et de la protection des dispositifs et systèmes de sécurité de Soins communs.

Le bureau d'assistance assigne l'événement au groupe de soutien pertinent en vue d'une enquête et d'un diagnostic plus approfondis. Le plan de RICS prévoit une classification des incidents de sécurité en fonction du niveau de risque, à savoir :

Un **fournisseur de services de sécurité gérés** est une entreprise technologique qui fournit des services de cybersécurité aux entreprises et aux organisations.

Source : Centre canadien pour la cybersécurité

Un **centre des opérations de sécurité** est une équipe de professionnels de la cybersécurité dédiée à la surveillance de l'infrastructure informatique d'une organisation 24h/24 et 7j/7. L'équipe est chargée de détecter, d'analyser et de répondre aux incidents de sécurité en temps réel.

Priorité critique

- Incident de cybersécurité, tel qu'une attaque par rançongiciel, qui perturbe les services de santé au point d'empêcher l'accès aux soins (p. ex., annulation de traitements contre le cancer, acheminement des patients vers d'autres territoires de compétence) ou aux services de santé OU d'une autre manière qui influe très négativement sur les résultats pour les patients.
- Incident de cybersécurité ayant un impact sur des services de santé au niveau provincial.
- Accès non autorisé à des données ou exfiltration de données susceptibles de causer un préjudice important à une personne, à des membres du public ou à des employés du secteur de la santé (p. ex., renseignements financiers).
- Accès non autorisé à des données ou exfiltration de données à grande échelle (p. ex., systèmes contenant un million de dossiers de patients individuels ou plus).
- Les auteurs de la menace ont compromis l'environnement au point que des mesures extrêmes (p. ex., mise hors ligne d'un centre de données, isolement du réseau d'un organisme de prestation de services, arrêt de systèmes ou de services informatiques essentiels) sont nécessaires pour maîtriser, corriger et résoudre l'incident et rétablir les services.

Priorité élevée

- Incident de cybersécurité qui perturbe les services de santé à un degré tel qu'il exerce une pression sur le système de santé en entravant considérablement les flux de travail pendant une période prolongée et/ou en retardant l'accès aux soins (p. ex., annulation de traitements contre le cancer, acheminement des patients vers d'autres territoires de compétence) ou aux services de santé OU d'une autre manière qui influe négativement sur les résultats pour les patients.
- Incident de cybersécurité ayant un impact sur des services de santé spécifiques à une région ou à un lieu donné.
- Accès non autorisé à des données ou exfiltration de données susceptibles de donner lieu à une violation de données rendue publique qui ne causera probablement pas de préjudice important (voir la définition de *la Loi sur les renseignements médicaux personnels*) à une personne ou à des membres du public.
- Les auteurs de la menace ont compromis l'environnement au point que les mesures nécessaires pour maîtriser, corriger et résoudre l'incident requièrent la mise hors ligne de systèmes non critiques ou de segments de réseau à faible impact.

Priorité moyenne

- L'incident de cybersécurité ne perturbe pas les services de santé.
- L'accès non autorisé aux données se limite aux éléments d'identification de l'utilisateur (p. ex., hameçonnage) ou à d'autres données non sensibles.
- L'événement est maîtrisé, corrigé et résolu dans le cadre des paramètres de fonctionnement prévus par les contrôles existants, mais il laisse penser qu'un auteur de menace ou un logiciel malveillant s'est infiltré dans l'environnement.

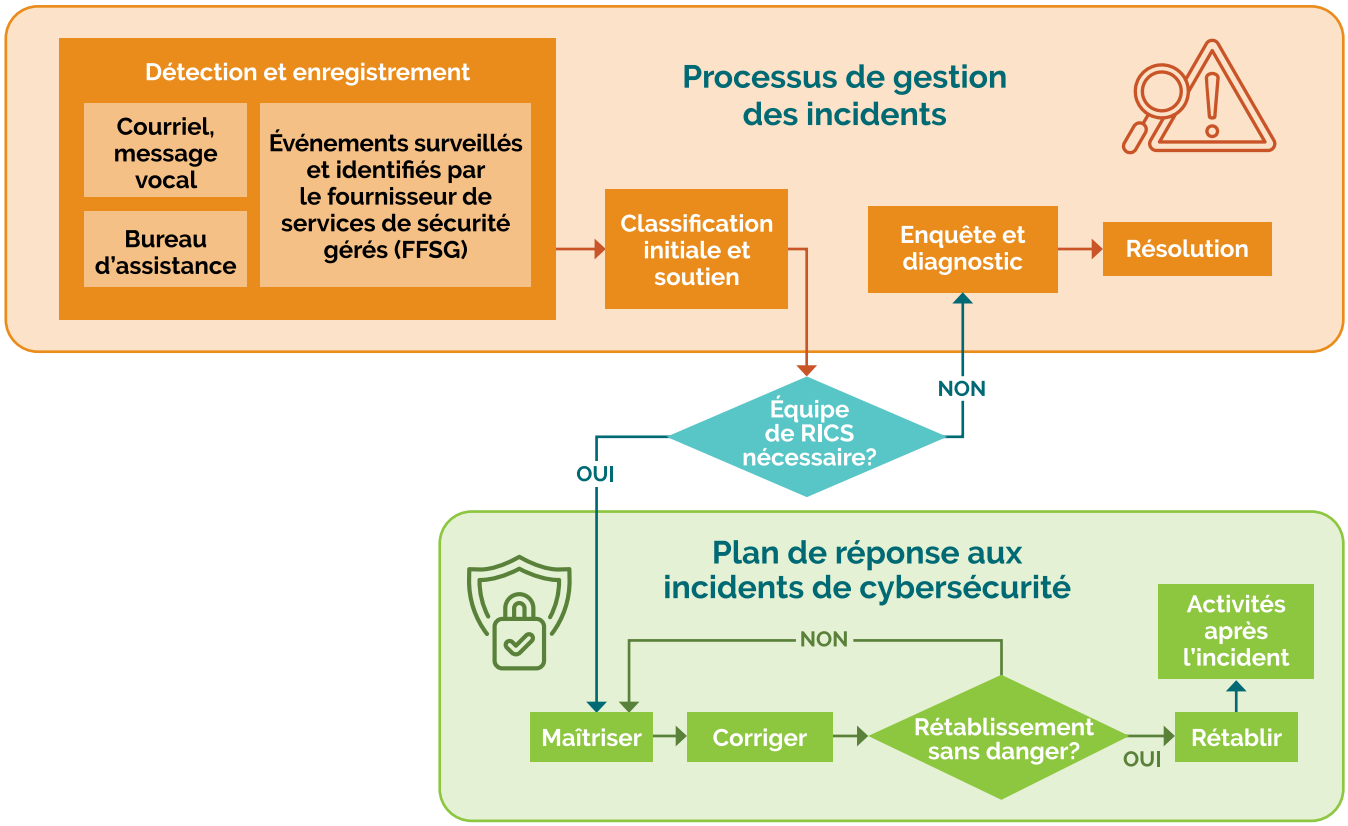
Priorité faible

- Les incidents classés comme faibles n'ont pas d'impact sur l'accès aux soins, les résultats pour les patients, les services de santé, les opérations de l'organisation, les actifs de l'organisation ou les personnes. L'événement est maîtrisé, corrigé et résolu dans le cadre des paramètres de fonctionnement prévus par les contrôles existants ou des procédures opérationnelles normalisées.

Source : Plan de réponse aux incidents de cybersécurité de Soins communs

Lorsqu'un événement est classé comme un incident de cybersécurité de priorité élevée ou critique, le plan de RICS est déclenché et l'équipe responsable de la RICS prend en charge le processus de gestion des incidents en vue de la résolution. L'interaction entre les deux processus est illustrée à la **FIGURE 2**:

Figure 2 : Interaction entre le processus de réponse aux incidents de cybersécurité et le processus de gestion des incidents à Soins communs



La composition et les responsabilités de l'équipe responsable de la RICS sont également définies dans le plan de RICS. De nature interfonctionnelle, cette équipe répond aux incidents de cybersécurité qui se produisent et est responsable de l'exécution du plan de réponse aux incidents. L'équipe comprend non seulement les techniciens qui interviennent en cas d'incident, mais aussi les personnes qui prennent des décisions opérationnelles ou juridiques en rapport avec l'incident. En outre, le plan de RICS fait des renvois au guide de gestion des incidents pour décrire les modes de réunions et de communications pour les activités de réponse aux incidents de cybersécurité.

Le plan ne s'applique pas aux événements indésirables causés par des catastrophes naturelles. Il ne s'applique qu'aux événements liés à la sécurité de l'information, p. ex. :

- **le déni de service;**
- la perte de renseignements sensibles (renseignements personnels sur la santé, renseignements permettant d'identifier une personne, etc.);
- les activités informatiques ou de réseau suspectes, y compris les courriels ou les escroqueries par **hameçonnage**, les **codes malveillants** et les **rançongiciels**;
- l'accès non autorisé à toute donnée ou tout système géré par Soins communs, y compris l'utilisation incorrecte ou inappropriée des systèmes ou des ressources du réseau.

Une attaque par **déni de service** est une cyberattaque qui dirige un grand volume de trafic Internet malveillant vers une cible, souvent un site Web ou un service connecté à Internet, afin de la saturer et de la neutraliser.
Source : Centre canadien pour la cybersécurité

L'**hameçonnage** est une tentative par un tiers de solliciter de l'information confidentielle auprès d'un individu, d'un groupe ou d'une organisation en usurpant ou en imitant une marque commerciale précise, généralement connue, dans le but de réaliser des gains financiers.
Source : Centre canadien pour la cybersécurité

Un **code malveillant** est un programme inséré dans un système, généralement de manière dissimulée, dans le but de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation de la victime.
Source : NIST SP1800-10B

Un **rançongiciel** est un type de maliciel (logiciel malveillant) qui bloque l'accès de l'utilisateur à des fichiers ou systèmes jusqu'au versement d'une somme d'argent.
Source : Centre canadien pour la cybersécurité

Cette page a été laissée
blanche intentionnellement.

Objectif, portée et approche, et critères d'audit(s)

Objectif

Déterminer si Soins communs dispose d'un processus permettant de répondre rapidement aux incidents de cybersécurité et d'en minimiser l'impact sur les opérations de santé et la perte de données.

Portée et approche

L'audit comprenait l'inspection des documents, des procédures, des normes, des rapports et d'autres documents relatifs au processus mis en œuvre par Soins communs pour gérer les incidents de cybersécurité touchant le système de santé provincial du Manitoba. Nous avons mené des entretiens avec des intervenants et des responsables de processus clés au sein des Services numériques partagés, qui relèvent de Soins communs, afin de comprendre les processus et les activités en place pour gérer les incidents de cybersécurité et y répondre.

Critères d'audit

Pour déterminer si Soins communs dispose d'un processus permettant de répondre rapidement aux incidents de cybersécurité et d'en minimiser l'impact sur les opérations de santé et la perte de données, nous avons appliqué les critères suivants :

Critères d'audit	Sources
Critères 1 : Une politique, des plans et des procédures de réponse aux incidents devraient être élaborés afin de détecter, d'analyser, de hiérarchiser, de maîtriser et d'atténuer les incidents de cybersécurité et de se rétablir.	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61r2: Computer Security Incident Handling Guide
Critères 2 : Des exercices sont organisés pour tester les plans de réponse aux incidents de sécurité et pour former le personnel à ses responsabilités en matière de gestion des incidents de sécurité.	
Critères 3 : Les incidents de sécurité sont gérés conformément à la politique, aux plans et aux procédures de réponse aux incidents.	

Cette page a été laissée
blanche intentionnellement.

Soins communs dispose d'un processus permettant de répondre rapidement aux incidents de cybersécurité, mais les tests réguliers et la formation peuvent être améliorés

La fiabilité et l'accessibilité des systèmes provinciaux d'information sur la santé sont essentielles pour fournir les services de santé qui influent directement la vie des gens. Cependant, ces systèmes sont très vulnérables aux cyberattaques – y compris aux rançongiciels et au vol de données – en raison de la multitude de renseignements sensibles personnels et liés à la santé qu'ils stockent. Les auteurs d'attaques savent que toute perturbation pourrait compromettre les soins aux patients, et les organismes de soins de santé peuvent se sentir contraints de payer les cybercriminels pour assurer le maintien de services vitaux et empêcher la vente ou l'exposition de renseignements sensibles.

Outre les incitations financières, un processus inadéquat de réponse aux incidents de cybersécurité et des contrôles mal conçus peuvent rendre les organismes incapables de gérer efficacement les incidents de sécurité et de se rétablir par la suite. Il peut en résulter des temps d'arrêt prolongés affectant de nombreux systèmes et entraînant de graves conséquences telles que l'incapacité à fournir des services médicaux essentiels, l'exposition de renseignements personnels liés à la santé, le recours forcé à des processus manuels et une atteinte importante à la réputation de l'organisme.

Dans le cadre de cet audit, nous avons constaté que Soins communs disposait de processus permettant de répondre rapidement aux incidents de cybersécurité et d'en minimiser l'impact sur les opérations de santé et la perte de données. Toutefois, des améliorations sont possibles, notamment en ce qui concerne les tests réguliers et la formation.

Notre conclusion s'appuie sur les constatations suivantes :

- La norme et le plan de réponse aux incidents de cybersécurité (RICS) sont en place, mais ils ne font pas l'objet d'une formation complète, et certaines pratiques à l'appui de la réponse aux incidents de cybersécurité ne sont pas encore documentées **(SECTION 1)**.
- Aucun exercice n'a été réalisé pour mettre à l'essai le plan de réponse aux incidents de cybersécurité **(SECTION 2)**.
- Des procédures sont en place pour déclencher le plan de RICS au besoin **(SECTION 3)**.

1 La norme et le plan de réponse aux incidents de cybersécurité sont en place, mais ils ne font pas l'objet d'une formation complète, et certaines pratiques à l'appui de la réponse aux incidents de cybersécurité ne sont pas encore documentées

La norme de sécurité relative à la réponse aux incidents de cybersécurité (RICS) à Soins communs exige l'existence d'un plan de RICS documenté, diffusé et approuvé. En février 2024, Soins communs a approuvé son plan de RICS, qui détaille le processus de réponse et de gestion des incidents de cybersécurité. Préparé par l'équipe de cybersécurité des Services numériques partagés, ce plan définit les incidents de cybersécurité.

Les incidents de cybersécurité sont traités en fonction de leur classification. Les incidents de priorité faible ou moyenne sont gérés par l'équipe de cybersécurité interne. En revanche, ceux de priorité élevée ou critique sont traités par l'équipe de Soins communs responsable de la RICS, une équipe interfonctionnelle chargée d'exécuter le plan de RICS en cas d'incidents de cybersécurité. Cette équipe compte notamment les membres et services suivants :

- des membres de la haute direction (p. ex., le chef de l'exploitation et des hauts dirigeants des Services numériques partagés et des organismes de prestation de services);
- le dirigeant principal de la sécurité de l'information;
- la direction des Services numériques partagés;
- les services de sécurité de l'information;
- des spécialistes de questions techniques (comme le soutien aux applications et aux serveurs);
- les services des ressources humaines;
- les services juridiques.

Soins communs a également recours à des ressources externes pour répondre aux incidents de cybersécurité, notamment un fournisseur de services de sécurité gérés (FSSG), qui propose des services de détection et d'analyse des événements de sécurité. En outre, la police d'assurance cybersécurité de Soins communs donne également accès à d'autres ressources, telles qu'un service d'accompagnement en cas de violation, des experts en criminalistique numérique et des conseillers juridiques, ce qui permet d'assurer un soutien complet en cas d'incident de cybersécurité.

La norme de RICS exige également que Soins communs enregistre les incidents de cybersécurité tout au long de leur cycle de vie. Pour se conformer à cette exigence, Soins communs utilise un outil de gestion des services de technologie de l'information (GSTI). Cet outil consigne les principaux détails tels que le numéro de dossier, les coordonnées de la personne qui signale l'incident, la description de l'incident, le niveau de priorité, les mesures prises et les détails de la résolution.

Nous avons constaté que Soins communs a progressé dans l'élaboration et la documentation de son plan de RICS. Néanmoins, les points suivants sont encore en cours ou n'ont pas été mis en œuvre à ce stade :

- Les responsabilités de l'équipe chargée de la RICS n'ont pas été communiquées à l'ensemble de l'équipe d'intervention.
- Le plan de communication externe et le guide sur les rançongiciels et les tentatives d'extorsion à l'intention des dirigeants étaient toujours en cours d'élaboration.
- Aucune politique de conservation des données probantes n'a été établie.

1.1 Les responsabilités établies dans le plan de réponse aux incidents de cybersécurité n'ont pas été communiquées à l'ensemble de l'équipe d'intervention

Soins communs dispose d'une norme de réponse aux incidents de cybersécurité, qui définit les exigences, les normes et les spécifications de base en matière de sécurité afin de garantir une réponse efficace aux incidents de sécurité de l'information. Cette norme définit également les exigences essentielles en matière de contrôle administratif et technique concernant la détection et la gestion des incidents de cybersécurité et la réponse à y apporter.

L'une des exigences de cette norme est la documentation, la communication et l'approbation d'un plan de réponse aux incidents de cybersécurité (RICS). Un plan de RICS documenté a certes été approuvé en février 2024, mais seuls certains membres de l'équipe de RICS, qui faisaient également partie de l'équipe de direction, ont été informés de leurs responsabilités. Il n'y a pas eu de séance spéciale – que ce soit dans le cadre d'une formation ou d'une mise à l'essai du plan – pour étudier le plan de RICS dans son intégralité avec l'ensemble de l'équipe responsable de la RICS. De ce fait, les rôles précis et les attentes spécifiques, qui diffèrent du contenu du guide de gestion des incidents plus largement diffusé, n'ont pas été communiqués.

Le fait de ne pas communiquer officiellement les procédures et les plans existants à l'équipe responsable de la RICS et de ne pas fournir à ses membres la formation nécessaire sur leurs rôles et responsabilités pourrait occasionner des retards dans la réponse aux incidents de cybersécurité à Soins communs.

Recommandation 1

Nous recommandons à Soins communs de mettre en œuvre des programmes de formation pour s'assurer que les membres de l'équipe responsable de la réponse aux incidents de cybersécurité comprennent bien leurs rôles et responsabilités spécifiques décrits dans le plan de réponse connexe.

1.2 Certaines pratiques à l'appui de la réponse aux incidents de cybersécurité ne sont pas encore documentées

La norme de réponse aux incidents de cybersécurité (RICS) de Soins communs exige que le plan de RICS inclue des considérations liées à la communication, en particulier pour les incidents de priorité élevée et critique où des contrôles de sécurité ont été contournés ou n'ont pas fonctionné. Actuellement, le guide de gestion des incidents décrit des protocoles et des processus de communication interne pour la gestion de ces incidents. Nous avons constaté qu'un plan de communication externe était encore au stade de l'élaboration. Une fois achevé, ce plan indiquera comment communiquer avec les intervenants externes (clients, fournisseurs, organismes d'application de la loi, médias, etc.), pendant et après un incident de cybersécurité.

La norme de RICS exige également que le plan de RICS soit étayé par des dossiers d'exploitation fournissant des lignes directrices en cas d'événements à risque élevé tels que les attaques par rançongiciel ou par déni de service. Un grand nombre de ces dossiers d'exploitation étaient en place. En outre, nous avons constaté que des guides avaient été préparés. Ces deux types de documents fournissent des instructions structurées et étayées pour guider les équipes dans leur réponse aux incidents, garantissant ainsi la cohérence et l'efficience de l'exécution. Toutefois, le guide sur les rançongiciels et les tentatives d'extorsion à l'intention des dirigeants était encore en cours d'élaboration. Un tel guide est essentiel, car il s'adresse aux cadres supérieurs et aux hauts dirigeants (directions générales, directions financières, équipes juridiques, etc.). Un guide sur les rançongiciels existe déjà, mais il est plutôt axé sur les conseils techniques et s'adresse aux équipes chargées de la sécurité de l'information et de la réponse aux incidents. En revanche, un guide distinct sur les rançongiciels et les tentatives d'extorsion à l'intention des dirigeants fournirait à la direction de Soins communs l'information nécessaire pour gérer les cas d'extorsion perturbateurs et l'aiderait à se préparer aux décisions à prendre dans des situations aussi stressantes.

Bien que Soins communs ait mis en place certaines mesures d'atténuation, telles que le guide de gestion des incidents, les dossiers d'exploitation existants et le service d'accompagnement proposé en cas de violation dans le cadre de leur police d'assurance cybersécurité, l'absence d'un plan de communication externe complet et l'élaboration inachevée du guide sur les rançongiciels et les tentatives d'extorsion à l'intention des dirigeants compromettent la capacité de l'organisation à répondre efficacement aux incidents de priorité élevée ou critique. En l'absence d'un plan de communication externe spécifique, il existe un risque de retard, de mauvaise communication et de mobilisation inadéquate des intervenants au cours des incidents de cybersécurité, ce qui pourrait entraver les efforts de réponse et avoir des conséquences sur la réputation de l'organisation. De plus, en s'appuyant uniquement sur le guide relatif aux rançongiciels, Soins communs s'expose à des risques stratégiques, financiers et d'atteinte à la réputation qu'une réponse purement technique ne serait pas en mesure de traiter. Le fait de disposer d'un guide distinct sur les rançongiciels et les tentatives d'extorsion à l'intention des dirigeants permettra à ces derniers d'être prêts à prendre des décisions éclairées tout en préservant la continuité des opérations et la confiance des intervenants.

Recommandation 2

Nous recommandons à Soins communs de parachever le plan de communication externe lié à la réponse aux incidents de cybersécurité ainsi que le guide sur les rançongiciels et les tentatives d'extorsion à l'intention des dirigeants. Une fois achevés, ces documents devraient être examinés avec les intervenants concernés.

1.3 Evidence retention policy not defined

Selon la publication spéciale 800-61r2 du National Institute of Standards and Technology (NIST) intitulée *Computer Security Incident Handling Guide*, il est important que tous les faits relatifs à un incident soient enregistrés immédiatement. Soins communs utilise son outil de gestion des services de technologie de l'information (GSTI) pour consigner les détails des incidents critiques, notamment le numéro de dossier, les coordonnées de la personne qui signale l'incident, la description de l'incident, le niveau de priorité, les mesures prises et les détails de la résolution.

La même norme du NIST exige également que les organisations établissent des politiques concernant la durée de conservation des données probantes liées à un incident. Nous avons constaté que les documents existants relatifs à la réponse aux incidents de cybersécurité (RICS) à Soins communs, y compris la norme de RICS, le plan de RICS et le guide de gestion des incidents, n'incluaient pas d'exigences particulières pour la conservation des données et des faits probants se rapportant aux incidents de cybersécurité.

En l'absence d'exigences clairement définies en matière de conservation des données et des faits probants liés aux incidents de cybersécurité, Soins communs pourrait être confronté à des difficultés pour préserver les renseignements essentiels nécessaires aux analyses judiciaires, aux procédures judiciaires ou au respect de la réglementation. Ce manque d'orientation pourrait entraîner la perte ou le mauvais traitement de données importantes liées aux incidents, ce qui se serait susceptible d'entraver les enquêtes, d'affaiblir la capacité de Soins communs à répondre à de futurs incidents et de l'exposer à des risques juridiques et réglementaires.

Recommandation 3

Nous recommandons à Soins communs d'établir une politique de conservation des données et des faits probants relatifs aux incidents de cybersécurité. Cette politique devrait définir la période de conservation, en tenant compte des exigences légales, des poursuites judiciaires possibles et des besoins organisationnels.

2 Aucun exercice n'a été réalisé pour mettre à l'essai le plan de réponse aux incidents de cybersécurité

Pour rester prêt à faire face aux incidents de cybersécurité, il faut non seulement disposer d'un plan de réponse, mais aussi s'assurer que ce plan est mis à l'essai régulièrement. La réalisation de tests concernant différents types d'incidents de cybersécurité – à l'aide de diverses méthodes d'essai telles que les exercices sur table et les tests fonctionnels – valide l'efficacité des procédures de réponse aux incidents et prépare les équipes à des scénarios réels.

La norme de réponse aux incidents de cybersécurité (RICS) de Soins communs exige que les plans de RICS soient examinés et/ou testés chaque année au moyen d'un exercice sur table. Nous avons constaté que Soins communs n'avait pas procédé à un examen ou à un exercice sur table du plan de RICS au cours de la période de vérification.

2.1 Le plan de réponse aux incidents de cybersécurité n'a pas été mis à l'essai

Selon la publication spéciale 800-84 du National Institute of Standards and Technology (NIST) intitulée *Guide to Test, Training and Exercise Programs for IT Plans and Capabilities*, même s'il faut disposer de plans visant à aider les organisations à répondre à diverses situations touchant les technologies de l'information (TI) et à les gérer, il est tout aussi important de maintenir l'actualité de ces plans. Il faut donc tester l'état de préparation du plan de RICS. Pour ce faire, ce plan peut être mis à l'essai afin de valider la capacité à exécuter les procédures de manière efficace et efficiente.

La mise à l'essai peut se faire des manières suivantes :

- Exercice sur table : Il s'agit d'un test fondé sur des discussions au cours duquel les participants examinent leurs rôles et les réponses à donner dans un scénario hypothétique de cybersécurité, et en discutent. Les actifs informatiques tels que le matériel ou les fichiers journaux des systèmes ne sont pas utilisés. Ce test aide les organisations à engager une discussion sur les rôles, les responsabilités, la coordination et la prise de décision entre les participants.
- Test fonctionnel : Ce test consiste à simuler un véritable scénario de cybersécurité, ce qui permet aux participants de jouer leur rôle en utilisant les procédures et les ressources informatiques comme ils le feraient lors de la réponse à un véritable incident de cybersécurité.

Ces deux types d'exercices sont essentiels pour garantir que les plans de réponse sont pratiques, complets et pertinents pour relever les défis réels de la cybersécurité.

Selon nos observations, la norme de réponse aux incidents de cybersécurité (RICS) exige de Soins communs qu'il examine et/ou mette à l'essai le plan de RICS chaque année à l'aide d'un exercice sur table. Il n'est pas nécessaire de procéder à un test fonctionnel du plan de RICS. Nous avons constaté que Soins communs n'avait effectué aucun test pour les divers scénarios d'incidents (rançongiciel, vol de données, attaques par déni de service, etc.).

Étant donné qu'aucun test n'a été effectué, l'efficacité du plan de RICS ne peut pas être évaluée pour garantir que Soins communs est prêt à répondre rapidement à un événement majeur en matière de cybersécurité.

Recommandation 4

Nous recommandons que Soins communs procède à des tests annuels du plan de réponse aux incidents de cybersécurité. Une stratégie de mise à l'essai devrait être établie et inclure différentes méthodes de test et divers types d'incidents afin de renforcer les capacités de réponse.

3 Des processus sont en place pour déclencher le plan de réponse aux incidents de cybersécurité en cas de besoin

Nous avons évalué la gestion par Soins communs de la réponse aux incidents de cybersécurité, sachant que seule la gestion des incidents de priorité élevée ou critique relève du plan de réponse aux incidents de cybersécurité (RICS). Nous avons observé que le processus global de gestion des incidents couvre la détection, l'enregistrement et la classification de tous les événements de sécurité. La classification est essentielle pour déterminer si la gestion d'un incident relèvera du plan de RICS et de l'équipe responsable de la RICS. D'avril 2022 à avril 2024, aucun incident de cybersécurité élevé ou critique n'a été signalé.

Étant donné qu'aucun incident de priorité élevée ou critique ne s'est produit au cours de la période d'audit, nous avons évalué les pratiques et les contrôles permettant de détecter, d'enregistrer et de hiérarchiser les événements de sécurité de priorité moyenne et faible à l'aide du processus de gestion des incidents. Tous les événements sont soumis à ce processus, et la classification des risques établit s'ils sont requalifiés en incidents de cybersécurité de priorité élevée ou critique nécessitant l'intervention de l'équipe responsable de la RICS. Nous avons constaté que les processus de gestion des incidents et de réponse aux incidents de cybersécurité concordent. Les phases de réponse aux incidents de cybersécurité de Soins communs comme la détection et l'analyse sont intégrées au processus de gestion des incidents de l'organisme, ce qui donne une approche claire en matière de classification et de gestion des incidents, minimise les risques pour le système de santé du Manitoba et facilite le rétablissement des services en temps opportun.

Cette page a été laissée
blanche intentionnellement.

Renseignements supplémentaires sur l'audit

Ce rapport de certification indépendant sur le processus de réponse et de gestion des incidents de cybersécurité de Soins communs a été préparé par le Bureau du vérificateur général du Manitoba (le Bureau). Notre responsabilité consistait à fournir des renseignements objectifs, des conseils et une certification pour aider l'Assemblée législative à vérifier la gestion des ressources et des programmes du gouvernement et à déterminer si Soins communs se conformait à tous les égards importants aux critères applicables.

Tout le travail de cet audit a été exécuté à un niveau de certification raisonnable, conformément à la Norme canadienne de missions de certification (NCMC) 3001 – Missions d'appréciation directe établie par les Comptables professionnels agréés du Canada (CPA Canada) dans le Manuel de CPA Canada – Certification.

Le Bureau applique la Norme canadienne de gestion de la qualité (NCGQ) 1 et est ainsi tenu de concevoir, de mettre en place et d'utiliser un système de gestion de la qualité, avec notamment des politiques et des procédures concernant la conformité avec les règles de déontologie, les normes professionnelles et les exigences législatives et réglementaires applicables.

Nous avons respecté les normes d'indépendance et autres règles déontologiques du code de conduite professionnelle de l'Ordre des comptables professionnels agréés du Manitoba, lesquelles reposent sur des principes fondamentaux d'intégrité, d'objectivité, de compétence et de diligence professionnelles, de confidentialité et de professionnalisme.

Conformément à notre processus d'audit habituel, nous avons obtenu ce qui suit de la part de la direction :

- la confirmation de la responsabilité de la direction quant à l'objet de l'audit;
- la reconnaissance de la validité des critères utilisés pour l'audit;
- la confirmation que tous les renseignements connus qui ont été demandés ou qui pourraient avoir une incidence sur les constatations ou la conclusion de l'audit ont été fournis.

Période visée par l'audit

L'audit visait la période allant d'avril 2022 à mars 2024. C'est la période à laquelle s'applique la conclusion de l'audit.

Date du rapport d'audit

Nous avons obtenu des éléments probants adéquats et appropriés sur lesquels fonder notre conclusion d'audit le 30 novembre 2024, à Winnipeg, au Manitoba.

Cette page a été laissée
blanche intentionnellement.

Résumé des recommandations et réponse des responsables

Recommandation 1

Nous recommandons à Soins communs de mettre en œuvre des programmes de formation pour s'assurer que les membres de l'équipe responsable de la réponse aux incidents de cybersécurité comprennent bien leurs rôles et responsabilités spécifiques décrits dans le plan de réponse connexe.

Réponse des responsables :

Soins communs est d'accord avec la possibilité d'améliorer nos pratiques actuelles tel que l'indique la recommandation. En réponse à cette recommandation, nous réalisons actuellement :

- un examen de cette version du plan de réponse aux incidents de cybersécurité (RICS) avec les principaux membres de l'équipe responsable de la RICS afin de s'assurer que ces personnes ont pris connaissance du plan et comprennent clairement leur rôle et leurs responsabilités;
- avec notre équipe des solutions de formation organisationnelles, l'élaboration d'un cours de formation relatif au plan de RICS qui sera accessible depuis notre système de gestion de l'apprentissage en ligne pour la formation continue.

Quant aux préoccupations liées au fait que les rôles précis et les attentes spécifiques diffèrent du contenu du guide de gestion des incidents plus largement diffusé, nous y répondons dans le cadre de l'élaboration de notre plan de communication externe sur la réponse aux incidents de cybersécurité et du guide sur les rançongiciels et les tentatives d'extorsion à l'intention des dirigeants, mentionnée dans la recommandation 2.

Recommandation 2

Nous recommandons à Soins communs de parachever le plan de communication externe lié à la réponse aux incidents de cybersécurité ainsi que le guide sur les rançongiciels et les tentatives d'extorsion à l'intention des dirigeants. Une fois achevés, ces documents devraient être examinés avec les intervenants concernés.

Réponse des responsables :

Soins communs est d'accord avec cette recommandation, et les deux documents associés à cette conclusion ont été parachevés. Les principaux intervenants ont été mis à contribution tout au long de l'élaboration du plan de communication externe et du guide sur les rançongiciels.

Même si le plan de communication externe et le guide sur les rançongiciels nous aideront dans nos activités de planification et de préparation, nous pensons que notre stratégie consistant à faire appel, dans le cadre de nos efforts de réponse aux incidents, à un service d'accompagnement

en cas de violation offert par notre assurance cybersécurité reste une mesure raisonnable d'atténuation de tous les risques associés à cette constatation.

Recommandation 3

Nous recommandons à Soins communs d'établir une politique de conservation des données et des faits probants relatifs aux incidents de cybersécurité. Cette politique devrait définir la période de conservation, en tenant compte des exigences légales, des poursuites judiciaires possibles et des besoins organisationnels.

Réponse des responsables :

Les Services numériques partagés sont d'accord avec la possibilité d'améliorer nos pratiques, tel que l'indique la recommandation, et ont mis à jour leur norme de réponse aux incidents de cybersécurité en y incluant des exigences de conservation conformément à la Loi sur les délais de prescription.

Recommandation 4

Nous recommandons que Soins communs procède à des tests annuels du plan de réponse aux incidents de cybersécurité. Une stratégie de mise à l'essai devrait être établie et inclure différentes méthodes de test et divers types d'incidents afin de renforcer les capacités de réponse.

Réponse des responsables :

Les Services numériques partagés sont d'accord avec la possibilité d'améliorer nos pratiques, tel que l'indique la recommandation, et nous prévoyons élaborer une stratégie pour examiner et mettre à l'essai notre plan de réponse aux incidents ainsi que la documentation à l'appui. Une fois la stratégie parachevée, nous établirons un calendrier régulier d'activités (p. ex., visites et exercices sur table) pour mettre à l'essai le plan de réponse aux incidents de cybersécurité.

Notre vision

Responsabilisation du gouvernement et excellence en administration publique au service des Manitobains.

Notre vission

Fournir de manière indépendante des renseignements, des conseils et des garanties concernant les activités du gouvernement et la gestion des fonds publics

Nos valeurs

Indépendance
Nous sommes indépendants du gouvernement et réalisons un travail objectif et impartial.

Intégrité
Nous agissons avec honnêteté et appliquons des normes déontologiques élevées.

Innovation
Nous mettons de l'avant l'innovation et la créativité dans nos activités et nos façons de faire.

Travail d'équipe
Nous travaillons en équipe en mettant en commun les connaissances et les compétences de chacun pour atteindre nos objectifs.

Vérificateur général
Tyson Shtykalo, FCPA, FCA

Vérificateur général adjoint, technologies de l'information et innovation
Wade Bo-Maguire

Directeur principal, Audit informatique
Ian Montefrio

Chef, Audit informatique
Arlene Nebrida

Auditeur principal, Audit informatique
Tony Chu

Chef, Analyse des données
Gabriel Nazario

Directeur des communications
Frank Landry

Soutien administratif
Tara MacKay
Alex Dela Cruz
Ivanna Romero

Conception graphique
Waterloo Design House

Le Bureau vérificateur général du Manitoba reconnaît avec respect que nous menons nos activités sur les terres ancestrales des nations anichinabé, anishininewuk, dakota oyate, dénésuline et nehethowuk, ainsi que sur le territoire national des Métis de la Rivière-Rouge. Nous respectons les traités conclus sur ces territoires, nous reconnaissons les préjudices et les erreurs du passé et nous nous engageons à aller de l'avant en partenariat avec les communautés autochtones dans un esprit de réconciliation et de collaboration.

VERSION DU SITE WEB

Vérificateur général
MANITOBA

Pour plus de renseignements, veuillez communiquer avec notre bureau :

Bureau du vérificateur général
330, avenue Portage, bureau 500
Winnipeg (Manitoba) R3C 0C4
Téléphone : 204 945-3790
contact@oag.mb.ca | www.oag.mb.ca/fr

@AuditorGenMB
@AuditorGenMB
@AuditorGenMB
company/manitoba-auditor-general