2025 RAPPORT DE LA VÉRIFICATRICE GÉNÉRALE DU CANADA AU PARLEMENT DU CANADA

La cybersécurité des réseaux et des systèmes du gouvernement

Bureau du vérificateur général du Canada
Office of the Auditor General of Canada

RAPPORT DE L'AUDITEUR INDÉPENDANT

Rapport d'audit de performance

Le présent rapport fait état des résultats d'un audit de performance réalisé par le Bureau du vérificateur général du Canada (BVG) en vertu de la Loi sur le vérificateur général.

Un audit de performance est une évaluation indépendante, objective et systématique de la façon dont le gouvernement gère ses activités et ses ressources et assume ses responsabilités. Les sujets des audits sont choisis en fonction de leur importance. Dans le cadre d'un audit de performance, le BVG peut faire des observations sur le mode de mise en œuvre d'une politique, mais pas sur le bien-fondé de celle-ci.

Les audits de performance sont planifiés, réalisés et présentés conformément aux normes professionnelles d'audit et aux politiques du BVG. Ils sont effectués par des auditrices compétentes et des auditeurs compétents qui :

- établissent les objectifs de l'audit et les critères d'évaluation de la performance;
- recueillent les éléments probants nécessaires pour évaluer la performance en fonction des critères;
- communiquent les constatations positives et négatives;
- tirent une conclusion en regard des objectifs de l'audit;
- formulent des recommandations en vue d'apporter des améliorations s'il y a des écarts importants entre les critères et la performance évaluée.

Les audits de performance favorisent une fonction publique soucieuse de l'éthique et efficace, et un gouvernement responsable qui rend des comptes au Parlement et à la population canadienne.

La publication est également diffusée sur notre site Web à l'adresse www.oag-bvg.gc.ca.

This publication is also available in English.

N° de catalogue FA1-27/2025-1-10F-PDF

ISBN 978-0-660-78927-9

ISSN 2561-3456

Photo de la page couverture : Olemedia/Gettyimages.ca

Survol

Message général

Dans l'ensemble, nous avons conclu que le gouvernement fédéral disposait d'outils pour protéger et défendre ses réseaux et ses systèmes contre les cyberattaques; toutefois, il y avait d'importantes lacunes dans les services de cybersécurité, la surveillance et les interventions lorsque des attaques se produisent. Au moment où les cyberattaques deviennent de plus en plus sophistiquées, répandues et graves, le gouvernement fédéral doit consolider continuellement ses mécanismes de défense.

La responsabilité de protéger les systèmes et opérations de technologie de l'information du gouvernement incombe conjointement au Secrétariat du Conseil du Trésor du Canada, au Centre de la sécurité des télécommunications Canada et à Services partagés Canada. Les organisations collaborent entre elles et avec les ministères et organismes pour prévenir le vol de données et limiter la perturbation des systèmes qui assurent la prestation de programmes et de services à la population canadienne. Toutefois, le fait que certaines organisations fédérales n'étaient pas assujetties aux mêmes politiques de sécurité a entraîné une utilisation incohérente des services de cybersécurité disponibles. Les lacunes dans les mécanismes de défense de cybersécurité empêchent le gouvernement de protéger les renseignements essentiels et de gérer les risques liés à la cybersécurité.

Pour protéger les réseaux et les systèmes fédéraux, le gouvernement doit également analyser les faiblesses potentielles de tous ses appareils, y compris les ordinateurs portables, les téléphones intelligents et les serveurs. Notre audit a révélé que Services partagés Canada et le Centre de la sécurité des télécommunications Canada ne disposaient pas d'un inventaire complet et à jour de tous les biens de technologie de l'information du gouvernement. En 2017, Services partagés Canada avait commencé à développer un projet de cybersécurité conçu pour fournir une vue complète des appareils dont dispose le gouvernement, mais le projet n'a pas été mené à terme. Faute de renseignements à jour sur les technologies de l'information à l'échelle de tous les ministères et organismes, le gouvernement fédéral risque de ne pas être bien informé des enjeux en matière de cybersécurité qui évoluent constamment, et encore moins d'y répondre rapidement.

Nous avons également constaté que la coordination entre les trois organisations n'était pas suffisante lorsque des attaques se produisaient. Par exemple, l'absence d'échange d'information a retardé la réponse du gouvernement à une cyberattaque majeure en janvier 2024, ce qui a permis au responsable de la cyberattaque d'accéder de façon prolongée à des renseignements personnels. Au moment de l'audit, aucun financement n'avait été accordé à une initiative visant à établir une plateforme de collaboration pour la cybersécurité et un outil de gestion des incidents.

Principales constatations et données clés

- D’avril 2023 à mars 2024, les capteurs au niveau du réseau du Centre de la sécurité des télécommunications Canada ont permis de bloquer quelque 2,4 billions d’événements de cybersécurité suspects, allant des simples balayages de réseaux aux cyberattaques sophistiquées.
- D’octobre 2023 à septembre 2024, le service Internet d’entreprise de Services partagés Canada a bloqué environ 6,6 billions d’événements de cybersécurité suspects.
- En juin 2024, Services partagés Canada a suspendu le projet de gestion de l’information et des incidents de sécurité. Cette initiative visait à cerner les événements de cybersécurité suspects et à déclencher automatiquement des interventions en cas de détection de cyberattaques.
- Dans le cadre du budget de 2024, le Secrétariat du Conseil du Trésor du Canada a reçu 11,1 millions de dollars sur 3 ans pour diriger la mise en œuvre d’une stratégie de cybersécurité. Nous avons constaté que cette stratégie, lancée en mai 2024, était solide et détaillée.

Les **Recommandations et réponses** se trouvent à la fin du présent rapport.

Table des matières

Introduction

Contexte

Sécuriser les réseaux et les systèmes du gouvernement contre les cyberattaques

1. Des cyberattaques (voir la pièce 1) se produisent désormais de manière fréquente au quotidien dans le monde. L'économie canadienne, l'infrastructure essentielle et la capacité du gouvernement fédéral de fournir des services à la population canadienne reposent de plus en plus sur les systèmes de technologie de l'information. Le Canada représente une cible intéressante pour les cyberattaques menées par des personnes qui cherchent à compromettre la sécurité nationale, la prospérité économique, le mode de vie des Canadiennes et des Canadiens et la confiance dans les institutions démocratiques.

2. Le gouvernement du Canada défend ses réseaux et ses systèmes contre de nombreuses cyberattaques quotidiennes. Cependant, la sophistication de ces dernières évolue aussi rapidement que la capacité du gouvernement à les prévenir et à intervenir. Les réseaux et les systèmes du gouvernement font parfois l'objet d'une atteinte à la sécurité, comme au Secrétariat du Conseil du Trésor du Canada et au ministère des Finances Canada en 2011 et au Conseil national de recherches Canada en 2014. Cette dernière atteinte a nui à la réputation de l'organisation, entraîné la perte de propriété intellectuelle, coûté au gouvernement environ 100 millions de dollars en mesures d'atténuation et donné lieu à un effort de plusieurs années pour reconstruire le réseau de l'organisation avec des mesures de cybersécurité appropriées.

3. Plus récemment, en janvier 2024, Affaires mondiales Canada a fait l'objet d'une cyberattaque d'une durée d'un mois qui a compromis son réseau et entraîné le vol de renseignements personnels. Enfin, en mars 2024, le Centre d'analyse des opérations et déclarations financières du Canada a été la cible d'une cyberattaque, ce qui a nécessité la mise hors ligne de certains de ses systèmes organisationnels. Voilà 2 des 1 017 événements de cybersécurité (voir la pièce 1) auxquels le Centre de la sécurité des télécommunications Canada a réagi pendant l'exercice 2023–2024.

Pièce 1 — Événement de cybersécurité, incident de cybersécurité et cyberattaque

Terme	Définition	Exemple
Événement de cybersécurité	• Dans un système ou un réseau, tout événement ou changement observable susceptible d'être pertinent sur le plan de la sécurité. • Les événements ne sont pas forcément synonymes d'atteinte à la sécurité ou de violation, mais peuvent devenir des incidents.	• Utilisatrice ou utilisateur qui se connecte à un système à une heure inhabituelle • Pare-feu qui bloque une connexion
Comprend ↓		
Incident de cybersécurité	• Événement non autorisé ou perturbateur qui nuit aux systèmes informatiques, aux réseaux ou aux données. • Cela comprend les événements intentionnels (malveillants) et non intentionnels (accidentels). • Les incidents de cybersécurité sont tous des événements, mais ne sont pas tous des attaques.	• Accès non autorisé à un système • Divulgation accidentelle de données
Comprend ↓		
Cyberattaque	• Acte délibéré et malveillant visant à accéder à des systèmes informatiques, à des réseaux ou à des appareils, à y créer des perturbations ou des dommages ou à y voler de l'information. • Toutes les cyberattaques constituent des incidents de cybersécurité.	• Attaque par rançongiciel • Attaque par déni de service • Vol de données

Source : D'après des renseignements du Centre de la sécurité des télécommunications Canada et du Secrétariat du Conseil du Trésor du Canada

Lire la description textuelle de la pièce 1

Rôles et responsabilités

4. **Secrétariat du Conseil du Trésor du Canada** — Le Secrétariat est chargé d'exercer un leadership stratégique ainsi que de fournir des conseils et des directives pour toutes les questions liées à la sécurité du gouvernement, y compris la cybersécurité. Il met en place et supervise une approche pangouvernementale en matière de gestion de la sécurité, en collaboration avec le Centre de la sécurité des télécommunications Canada et Services partagés Canada, et assure la surveillance et la coordination des politiques stratégiques pour les activités de gestion de la sécurité du gouvernement. Au sein du Secrétariat, le Bureau du dirigeant principal de l'information est responsable de diriger et de soutenir la mise en œuvre de la stratégie intégrée de cybersécurité du gouvernement fédéral.

5. **Centre de la sécurité des télécommunications Canada** — Cet organisme est responsable de la protection et de la défense des réseaux et des systèmes du gouvernement ainsi que de l'atténuation des répercussions des cyberattaques. Au sein de l'organisme, le Centre canadien pour la cybersécurité a été créé en 2018 pour veiller à la sécurité des réseaux et des systèmes du gouvernement, ainsi que des infrastructures essentielles du Canada présentant une importance pour le gouvernement fédéral. Le Centre constitue la source unique et centralisée de conseils, de directives, de services et de soutien spécialisés en cybersécurité pour le gouvernement, les propriétaires et gestionnaires d'infrastructures essentielles, le secteur privé et le public canadien.

6. **Services partagés Canada** — Ce ministère est responsable de la planification, de la conception, de la construction, de l'exploitation et de la maintenance d'une infrastructure et de services informatiques efficaces, efficients et adaptés, notamment la prestation de services de cybersécurité visant à sécuriser les réseaux et les systèmes du gouvernement sous sa responsabilité.

Objet de l'audit

7. Cet audit visait à déterminer si le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des télécommunications Canada et Services partagés Canada disposaient des outils nécessaires pour protéger et défendre de façon coordonnée les réseaux et les systèmes du gouvernement contre les cyberattaques.

8. Cet audit est important parce que dans un contexte de cyberattaques de plus en plus sophistiquées, fréquentes et dommageables, les mesures de protection du gouvernement

fédéral doivent évoluer continuellement afin d'assurer la protection efficace de ses réseaux et systèmes, qui contiennent notamment des renseignements de nature délicate et des renseignements personnels des Canadiennes et Canadiens.

9. La section intitulée **À propos de l'audit**, à la fin du présent rapport, donne des précisions sur l'objectif, l'étendue, la méthode et les critères de l'audit.

Constatations et recommandations

Une stratégie était en place pour gérer la cybersécurité

Importance de cette constatation

10. Cette constatation est importante parce que la gestion des risques liés à la cybersécurité nécessite une stratégie de cybersécurité solide et complète axée sur le gouvernement fédéral. Une stratégie définit la vision et les objectifs du gouvernement et précise les initiatives nécessaires pour renforcer la cybersécurité des réseaux et des systèmes du gouvernement.

Une nouvelle stratégie a orienté les activités de cybersécurité du gouvernement

Constatations

11. Le budget de 2024 prévoyait 11,1 millions de dollars sur 3 ans, à compter de l'exercice 2024-2025, pour que le Secrétariat du Conseil du Trésor du Canada pilote la mise en œuvre d'une stratégie de cybersécurité. Nous avons constaté qu'en mai 2024, le Secrétariat a lancé la Stratégie intégrée de cybersécurité du gouvernement du Canada pour renforcer la cybersécurité dans l'ensemble des opérations du gouvernement. Elle visait également à préserver la confiance des Canadiennes et des Canadiens quant au fait que leurs renseignements personnels dont dispose le gouvernement étaient protégés et que la prestation des programmes et services gouvernementaux ne serait pas interrompue. Nous avons constaté que cette stratégie était solide et complète. Elle faisait état de lacunes en matière de cybersécurité qui touchaient les réseaux et les systèmes gouvernementaux, et présentait des objectifs accompagnés de mesures clés et de résultats mesurables attendus afin d'y remédier (voir la pièce 2).

Pièce 2 — Objectifs et mesures clés de la Stratégie intégrée de cybersécurité du gouvernement du Canada

Vision	Objectifs de la stratégie	Exemples de mesures clés*
« Construire un gouvernement fédéral de classe mondiale, durable et résilient pour réduire les risques liés à la cybersécurité afin que les ministères et les organismes puissent fournir des services numériques sûrs et fiables. » **Mise en œuvre :** • Secrétariat du Conseil du Trésor du Canada • Centre de la sécurité des télécommunications Canada • Services partagés Canada • Ministères et organismes	**Expliquer clairement les risques liés à la cybersécurité et leur incidence sur les opérations**	• Établir un programme pangouvernemental de conformité et d'assurance pour évaluer les mécanismes de défense ministériels en matière de cybersécurité afin de cerner les risques de cybersécurité et d'en établir les priorités. • Créer un programme pangouvernemental de gestion des vulnérabilités afin de gérer et de réduire les vulnérabilités qui touchent les systèmes et les réseaux du gouvernement.
	Prévenir les cyberattaques et y résister plus efficacement	• Déployer les mécanismes de défense en matière de cybersécurité dans les petits ministères et organismes. • Établir un cadre permettant de mieux détecter et prévenir les activités frauduleuses visant les applications gouvernementales.
	Renforcer les capacités et la résilience à l'échelle du gouvernement du Canada	• Établir un cadre permettant aux ministères de tenir des inventaires exacts des applications et systèmes du gouvernement. Mener tout au long de l'année des essais et des examens de la protection et des mécanismes de défense en matière de cybersécurité. • Mettre en place une plateforme pangouvernementale de collaboration en matière de cybersécurité afin de gérer les événements de cybersécurité et d'y répondre.
	Établir un effectif fédéral diversifié et doté des compétences nécessaires en cybersécurité	• Développer les talents en matière de cybersécurité grâce à des programmes de formation interfonctionnelle. • Favoriser une culture de gestion des talents afin de recruter et de retenir des candidats qualifiés.

* La stratégie comporte de nombreuses autres mesures. Les exemples énoncés ici représentent une partie des mesures ayant une portée pangouvernementale.

Source : D'après des renseignements contenus dans la Stratégie intégrée de cybersécurité du gouvernement du Canada, Secrétariat du Conseil du Trésor du Canada, 2024

Lire la description textuelle de la pièce 2

Des services de cybersécurité étaient mis à la disposition des organisations fédérales pour les protéger, mais certaines ne les utilisaient pas

Importance de cette constatation

12. Cette constatation est importante parce que l'utilisation variable des services de cybersécurité fragmente l'environnement de cybersécurité du gouvernement fédéral. Cela complique son atténuation des risques liés à la cybersécurité et augmente donc la probabilité d'être victime de cyberattaques pouvant entraîner des dommages importants, comme le vol de renseignements personnels ou de nature délicate, le refus d'accès aux services et des pertes financières.

Des services de cybersécurité efficaces ont été développés pour protéger les réseaux et les systèmes du gouvernement

Constatations

13. Nous avons constaté que le Centre de la sécurité des télécommunications Canada avait conçu et proposé des capteurs de défense de cybersécurité pour détecter et atténuer les événements de cybersécurité, les incidents de cybersécurité et les cyberattaques (voir la pièce 3). Ces capteurs ajoutent une couche de cybersécurité aux services fournis par Services partagés Canada ou aux services de cybersécurité disponibles sur le marché, comme les logiciels antivirus et pare-feu.

14. Nous avons constaté que les capteurs au niveau du réseau avaient bloqué en moyenne 6,6 milliards d'événements de cybersécurité suspects par jour entre le 1er avril 2023 et le 31 mars 2024, ce qui représente un total annuel d'environ 2,4 billions. Ces événements de cybersécurité allaient des balayages de réseaux gouvernementaux aux cyberattaques sophistiquées. L'efficacité des capteurs de défense de cybersécurité du Centre de la sécurité des télécommunications Canada est reconnue dans le monde entier. Le gouvernement du Royaume-Uni a adopté certains de ces capteurs pour améliorer sa propre cybersécurité.

Pièce 3 — Le Centre de la sécurité des télécommunications Canada a conçu trois types de capteurs de défense de cybersécurité pour détecter et atténuer les événements de cybersécurité et les cyberattaques

Capteurs de défense de cybersécurité	Mis en œuvre	Description
Capteur au niveau du réseau 	2010	Détection et atténuation des incidents de cybersécurité sur les réseaux du gouvernement. Ce capteur est habituellement intégré au service Internet d'entreprise de Services partagés Canada.
Capteur au niveau de l'hôte 	2012	Détection des cyberattaques sur les points d'extrémité tels que les ordinateurs portables, les serveurs et les réseaux locaux. Le capteur analyse et traite l'information recueillie afin de détecter des événements de cybersécurité suspects survenant sur un appareil hôte. L'information recueillie sert à signaler les anomalies et les faiblesses aux organisations fédérales concernées.
Capteur infonuagique 	2019	Exploitation dans l'infrastructure infonuagique des organisations fédérales de pair avec les mécanismes de défense des fournisseurs de services infonuagiques. Le capteur automatise la collecte de l'activité consignée dans le nuage et analyse l'information afin de détecter et d'atténuer les événements de cybersécurité suspects.

Source : D'après des renseignements du Centre de la sécurité des télécommunications Canada

Lire la description textuelle de la pièce 3

15. Nous avons constaté que Services partagés Canada propose le service Internet d'entreprise, qui offre une connectivité sécurisée aux utilisatrices et aux utilisateurs du gouvernement fédéral pour accéder à Internet et à la population canadienne pour accéder aux sites Web du gouvernement. Le service Internet d'entreprise comprend une cybersécurité améliorée, soit la surveillance du trafic Internet et le blocage d'événements de cybersécurité suspects. Il intègre également les capteurs de défense de cybersécurité au niveau du réseau du Centre de la sécurité des télécommunications Canada (voir la pièce 3). Entre le 1er octobre 2023 et le 30 septembre 2024, le service Internet d'entreprise a bloqué en moyenne 18 milliards d'événements de cybersécurité suspects par jour, pour un total annuel d'environ 6,6 billions d'événements.

Tous les ministères, organismes et sociétés d'État n'utilisaient pas les services de cybersécurité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada

Constatations

16. Au moment de notre audit, le gouvernement du Canada était composé de 204 **organisations fédérales**[1]. Quatre-vingt-cinq de ces organisations, dont la plupart des grands ministères, étaient assujetties à des politiques du Conseil du Trésor les obligeant à utiliser le service Internet d'entreprise de Services partagés Canada et les capteurs de défense de cybersécurité du Centre de la sécurité des télécommunications Canada. Nous avons constaté que ces 85 organisations fédérales utilisaient toutes des capteurs de défense de cybersécurité, mais que 22 d'entre elles (soit 26 %) n'utilisaient pas le service Internet d'entreprise.

17. Aucune des 119 autres organisations fédérales n'était assujettie à ces politiques du Conseil du Trésor et donc tenue de recourir à ces services de cybersécurité. Cependant, le Secrétariat du Conseil du Trésor du Canada les encourageait fortement à le faire. Nous avons constaté que la majorité de ces 119 organisations fédérales n'avaient pas recours au service Internet d'entreprise de Services partagés Canada, mais la plupart utilisaient les capteurs de défense de cybersécurité du Centre de la sécurité des télécommunications Canada (voir la pièce 4).

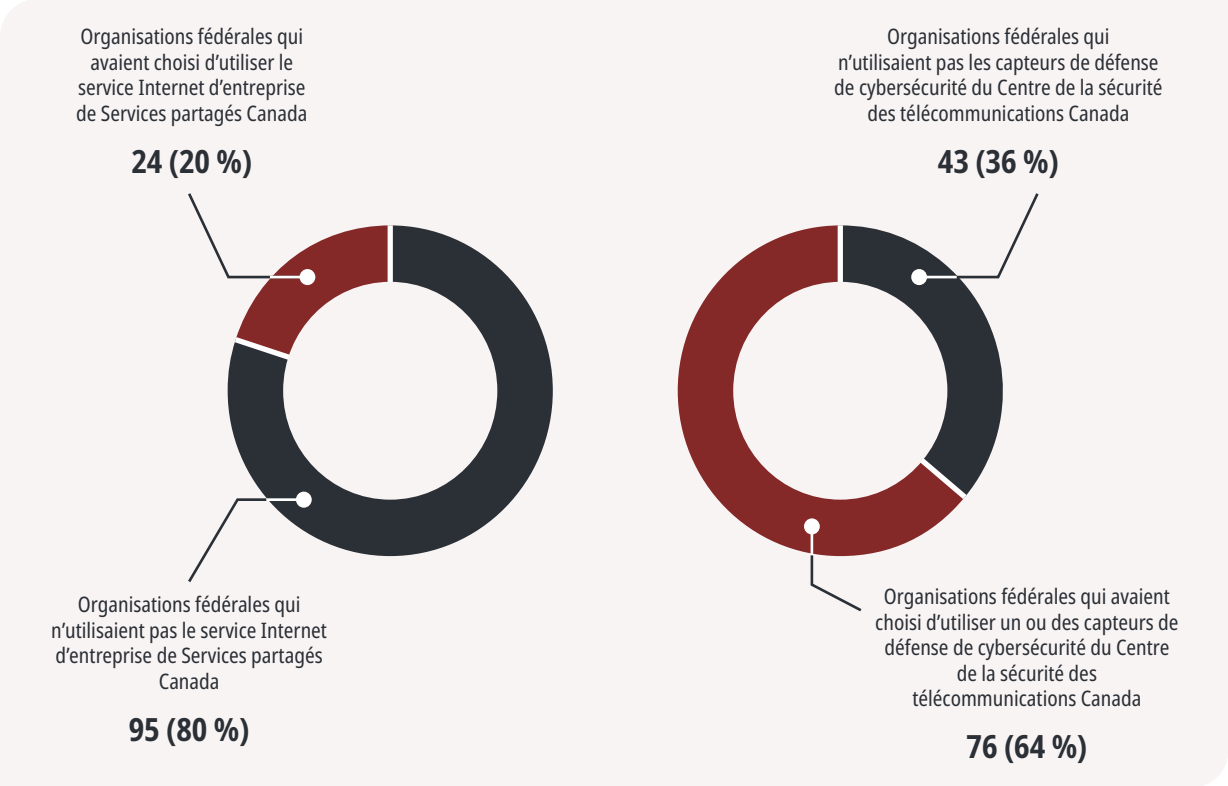
18. Des responsables du Centre de la sécurité des télécommunications Canada nous ont dit que le déploiement variable des capteurs de défense de cybersécurité à l'échelle des organisations fédérales avait créé des lacunes en matière de cybersécurité, ce qui limitait sa capacité à défendre les réseaux, les systèmes et les appareils du gouvernement.

19. Nous avons consulté 13 organisations fédérales (sociétés d'État et petits ministères et organismes) qui ne sont pas tenues de recourir aux services de cybersécurité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada afin de comprendre pourquoi elles n'y recouraient pas. Les préoccupations suivantes ont été mentionnées :

- Le recours à ces services de cybersécurité pouvait être perçu comme une menace pour l'indépendance des sociétés d'État.

1 **Organisations fédérales** — Ministère ou organisme fédéral, société d'État ou entité fédérale (conseil, commission, secrétariat, agent du Parlement, tribunal administratif, etc.) instauré par le gouvernement du Canada ou le Parlement afin d'assumer des responsabilités fédérales. Chaque type d'organisation est régi par des lois et peut être tenu ou non de respecter les politiques du Conseil du Trésor.

Pièce 4 — Les 119 organisations fédérales qui n'étaient pas tenues de recourir aux services de cybersécurité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada étaient encouragées à y recourir, mais beaucoup ont choisi de ne pas le faire



Source : D'après des données de Services partagés Canada et du Centre de la sécurité des télécommunications Canada

Lire la description textuelle de la pièce 4

- La capacité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada à adapter leurs services de cybersécurité aux besoins de ces organisations fédérales est limitée.
- Services partagés Canada et le Centre de la sécurité des télécommunications Canada pourraient améliorer le soutien et la maintenance de leurs services de cybersécurité.

20. Les réseaux et les systèmes des sociétés d'État et des petits ministères et organismes contiennent de l'information de nature délicate ainsi que les renseignements personnels des Canadiennes et des Canadiens. Nous estimons qu'en n'utilisant pas les services de cybersécurité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada, les organisations ont refusé un moyen de défense solide et reconnu qui pourrait renforcer leur protection actuelle. Cette protection supplémentaire comprend la défense contre des cyberattaques extrêmement sophistiquées

que des services de cybersécurité disponibles sur le marché pourraient ne pas détecter. Le fait de ne pas recourir aux services nuit également à la capacité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada de défendre les réseaux et les systèmes du gouvernement fédéral à plus grande échelle.

Les outils de surveillance et d'intervention en cas de cyberattaques présentaient des lacunes importantes

Importance de cette constatation

21. Cette constatation est importante parce que les lacunes dans la cybersécurité des réseaux et des systèmes du gouvernement ainsi que l'intervention tardive en cas de cyberattaque augmentent la probabilité de réussite des cyberattaques. Or les vols de renseignements personnels ou de nature délicate et les dommages aux systèmes de technologie de l'information peuvent avoir des répercussions sur la prestation de programmes et de services à la population canadienne. La clé d'une cybersécurité solide est de disposer des bons outils et des bonnes procédures connexes pour surveiller les événements de cybersécurité suspects et les incidents afin de prévenir les cyberattaques et d'intervenir efficacement lorsqu'une cyberattaque se produit.

Il y avait une lacune dans la surveillance des événements de cybersécurité suspects touchant les réseaux et les systèmes du gouvernement

Constatations

22. En avril 2017, Services partagés Canada a commencé à mettre au point une application de gestion de l'information et des événements de sécurité, qui devait être prête en mars 2023. La nouvelle application devait permettre d'avoir connaissance des événements de cybersécurité suspects touchant les réseaux et les systèmes gouvernementaux, être gérée par le Ministère et déclencher des interventions automatisées en cas de détection de cyberattaques. Une fois conçue et mise en œuvre correctement, la nouvelle application devait également améliorer la capacité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada de prédire et d'anticiper les cyberattaques sophistiquées et de réduire le temps qui s'écoule entre la détection et l'intervention.

23. Le budget initial du projet de mise au point de l'application s'élevait à 72,7 millions de dollars; après révision, il est passé à 144,3 millions de dollars en mai 2021. Nous avons constaté que le projet avait été retardé pour plusieurs raisons, notamment des difficultés à trouver et à sélectionner un fournisseur qualifié. Le projet a été mis en suspens en juin 2024 en attendant l'approbation d'un financement supplémentaire.

24. Le retard accusé par le projet a empêché de régler les lacunes existantes en matière de surveillance de la cybersécurité et engendré des pratiques inefficaces. Nous avons constaté ce qui suit :

- Services partagés Canada n'était pas en mesure de surveiller tous les événements de cybersécurité suspects touchant les réseaux, les systèmes et les appareils du gouvernement sous sa responsabilité.
- En ce qui concerne les événements de cybersécurité dont l'analyse relevait du Centre de la sécurité des télécommunications Canada, Services partagés Canada n'informait ce dernier que d'une partie des événements pour en permettre l'analyse. L'organisme a indiqué que l'analyse de ces événements de cybersécurité suspects avait coûté environ 16,9 millions de dollars au total pour les trois exercices allant de 2021-2022 à 2023-2024, et que le coût pour l'exercice 2024-2025 était estimé à 13,8 millions de dollars. Des responsables du Centre de la sécurité des télécommunications Canada nous ont indiqué qu'ils s'attendaient à ce que les coûts continuent d'augmenter et que l'organisme avait besoin de ressources supplémentaires pour poursuivre cette analyse à l'avenir.

Recommandation

25. Services partagés Canada, en collaboration avec le Centre de la sécurité des télécommunications Canada, devrait établir un plan d'action clair comprenant des critères définis et un échéancier pour mettre au point une application de gestion de l'information et des événements de sécurité qui corrige les lacunes existantes en matière de surveillance de la cybersécurité.

Réponse du Ministère — Recommandation acceptée.

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Les inventaires centraux des biens de technologie de l’information du gouvernement étaient incomplets, ce qui augmentait le risque de cyberattaques

Constatations

26. Nous avons constaté que Services partagés Canada et le Centre de la sécurité des télécommunications Canada ne disposaient pas d’inventaires complets des biens de technologie de l’information exploités par les organisations fédérales qu’ils desservaient. Ces biens comprenaient les réseaux locaux et les points d’extrémité tels que les ordinateurs portables, les imprimantes et les serveurs. Plus précisément, nous avons constaté ce qui suit :

- Puisque Services partagés Canada ne disposait pas d’un inventaire central complet des réseaux ou des systèmes dont il est responsable, il n’avait pas une compréhension approfondie des réseaux et systèmes, y compris les logiciels de soutien, qui avaient besoin de correctifs, de mises à jour ou d’entretien, ou qui n’étaient plus pris en charge par le fournisseur.
- Le Centre de la sécurité des télécommunications Canada n’avait pas obtenu un inventaire central complet de tous les points d’extrémité des organisations fédérales qu’il desservait. À la fin de septembre 2024, les capteurs au niveau de l’hôte étaient installés sur environ 770 000 points d’extrémité. Cependant, certains points d’extrémité n’étaient pas munis des capteurs de l’organisme.

27. Le fait de ne pas avoir d’inventaire complet des biens de technologie de l’information nuisait à la capacité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada d’appuyer les organisations fédérales qu’ils desservent et de gérer les risques de cybersécurité pour les réseaux et systèmes du gouvernement. À cause de cet inventaire incomplet, il était également difficile pour le ministère et l’organisme de bien comprendre les biens de technologie de l’information utilisés par les organisations fédérales et leurs vulnérabilités intrinsèques susceptibles d’être exploitées lors d’une cyberattaque.

28. Nous avons constaté que les retards de son projet Visibilité, sensibilisation et sécurité de point d’extrémité empêchaient Services partagés Canada d’obtenir l’inventaire complet des biens de technologie de l’information dont il est responsable. Le projet, entamé en novembre 2017, devait être terminé en septembre 2024 et disposait d’un budget de 174,8 millions de dollars. Cependant, à la fin de la période visée par l’audit, le 30 septembre 2024, le projet était encore en cours en raison de diverses difficultés, y compris des changements apportés aux exigences du Ministère. Des

responsables de Services partagés Canada nous ont indiqué que le projet prendrait au moins trois années supplémentaires pour être achevé, soit jusqu'en 2027.

29. Nous avons constaté qu'en août 2024, le Secrétariat du Conseil du Trésor du Canada avait publié une directive concernant la politique sur la sécurité afin de renforcer la cybersécurité des réseaux et des systèmes du gouvernement. Entre autres exigences, les 85 organisations fédérales tenues de recourir aux services du Centre de la sécurité des télécommunications Canada avaient jusqu'à la mi-novembre 2024 pour confirmer à l'organisme que des capteurs de défense de cybersécurité (voir la pièce 3) avaient été installés sur tous ses points d'extrémité. À la fin de notre période d'audit, cette initiative était encore en cours.

Recommandation

30. Services partagés Canada devrait :

- s'assurer de disposer d'un inventaire central à jour des réseaux et des systèmes qu'il dessert dans l'ensemble des organisations fédérales, ainsi que d'un processus pour gérer les appareils qui ont besoin de correctifs, de mises à jour ou d'entretien, ou qui doivent être remplacés. Le Ministère devrait installer les correctifs requis, apporter les mises à jour nécessaires et assurer l'entretien et le remplacement des réseaux et des systèmes en conséquence;
- déterminer une solution aux difficultés auxquelles se heurte le projet Visibilité, sensibilisation et sécurité de point d'extrémité.

Réponse du Ministère — Recommandation acceptée.

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Recommandation

31. Le Secrétariat du Conseil du Trésor du Canada, en consultation avec le Centre de la sécurité des télécommunications Canada, devrait s'assurer que les organisations fédérales :

- installent des capteurs de défense de cybersécurité sur tous les points d'extrémité afin de repérer les vulnérabilités;
- corrigent rapidement les vulnérabilités.

Réponse du Secrétariat — Recommandation acceptée.

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Les procédures et protocoles de coordination et d'échange d'information concernant les cyberattaques étaient incomplets et il n'y avait aucun outil pour favoriser une coordination et une collaboration harmonieuses

Constatations

32. L'intervention en cas de cyberattaques contre les organisations fédérales est encadrée par le Plan de gestion des événements de cybersécurité du gouvernement du Canada, qui a été préparé par le Secrétariat du Conseil du Trésor du Canada. Bien que le Secrétariat ait dirigé la création du plan, il partage avec le Centre de la sécurité des télécommunications Canada et Services partagés Canada la responsabilité de mettre en place des procédures et des protocoles de coordination et d'échange d'information entre eux et entre les organisations fédérales lors des interventions en cas de cyberattaques. Toutefois, nous avons constaté que les procédures et protocoles de coordination et d'échange d'information étaient incomplets, ce qui retarde la réponse à une cyberattaque (voir la pièce 5).

Pièce 5 — Des lacunes en matière de coordination et d'échange d'information ont empêché de répondre rapidement à une cyberattaque

Récemment, lors d'une cyberattaque majeure contre une organisation fédérale, l'intervention du gouvernement a été retardée par des problèmes de coordination et de transmission de ressources et de renseignements de nature délicate.

- Lors de la réponse initiale à la cyberattaque, il était urgent que Services partagés Canada fournisse des renseignements clés de nature délicate au Centre de la sécurité des télécommunications Canada pour déterminer le niveau de menace et la source de la cyberattaque en cours. Toutefois, les procédures et protocoles d'échange étant incomplets, il a fallu sept jours pour demander et transmettre les renseignements, ce qui a retardé l'intervention lors de la cyberattaque.
- Plusieurs fois au cours de la cyberattaque, l'organisation fédérale visée a eu de la difficulté à joindre des experts en la matière à Services partagés Canada pour obtenir un soutien technique urgent.

L'intervention tardive a donné aux responsables de la cyberattaque plus de temps pour accéder aux renseignements du personnel détenus par l'organisation fédérale. Nous estimons que l'intervention du gouvernement aurait été plus rapide si des procédures et des protocoles complets de coordination et d'échange d'information avaient été en place.

33. Nous avons également constaté qu'il n'existait aucun outil de coordination qui favoriserait une collaboration et un échange d'information harmonieux pour assurer la prise rapide de décisions et de mesures en réponse à une cyberattaque. Au cours de notre

audit, nous avons examiné les rapports postérieurs à l'événement de huit cyberattaques survenues entre les années civiles 2022 et 2024 qui avaient touché diverses organisations fédérales. Nous avons constaté des problèmes récurrents quant aux capacités d'échange d'information entre toutes les organisations fédérales qui ont participé à l'intervention lors de ces attaques; nous avons également constaté qu'il n'existait aucun outil de collaboration pour faciliter l'échange d'information.

34. Conformément à la Stratégie intégrée de cybersécurité du gouvernement du Canada, le Centre de la sécurité des télécommunications Canada devait mettre en place une plateforme pangouvernementale de collaboration en matière d'événements de cybersécurité et un outil de gestion des incidents pour favoriser une collaboration et un échange d'information harmonieux en cas de cyberattaques. Nous avons constaté que l'organisme ne disposait d'aucun calendrier de mise en œuvre et n'avait pas fait de demande de financement pour cet outil. Des responsables du Centre de la sécurité des télécommunications Canada ont reconnu que la capacité du gouvernement à collaborer efficacement et à assurer la coordination dans le cadre d'une cyberattaque serait touchée jusqu'à ce que cette initiative soit mise en œuvre. À la fin de la période visée par l'audit, ces responsables nous ont indiqué que des travaux étaient en cours afin de préparer une demande de financement pour l'outil.

Recommandation

35. Le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des télécommunications Canada et Services partagés Canada devraient réévaluer leurs pratiques de gestion des incidents de cybersécurité pour améliorer la coordination et favoriser la communication rapide de l'information essentielle requise pour intervenir lors de cyberattaques visant des organisations fédérales.

Réponse des trois entités — Recommandation acceptée.

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Recommandation

36. Le Centre de la sécurité des télécommunications Canada devrait parachever sa demande de financement et prioriser ses travaux d'élaboration et de mise en œuvre d'une plateforme de collaboration en matière d'événements de cybersécurité et d'un outil de gestion des incidents. La nouvelle plateforme et le nouvel outil devraient permettre de normaliser la communication, le suivi,

la surveillance et la consignation des événements de cybersécurité; le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada et d'autres organisations fédérales devraient pouvoir y accéder.

Réponse de l'organisme — Recommandation acceptée.

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Conclusion

37. Nous avons conclu que le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des télécommunications Canada et Services partagés Canada disposaient des outils nécessaires pour protéger et défendre les réseaux et les systèmes du gouvernement contre les cyberattaques. Toutefois, la coordination et l'échange d'information pendant une cyberattaque comportaient des lacunes, et certains outils devaient être développés ou mis au point pour améliorer la capacité du gouvernement à répondre aux cyberattaques.

38. Bon nombre d'organisations fédérales ne sont pas tenues d'utiliser les services de cybersécurité offerts par le Centre de la sécurité des télécommunications Canada et Services partagés Canada et n'y ont pas recours. L'utilisation inégale de ces services a empêché le gouvernement d'être bien informé des événements de cybersécurité à l'échelle de la fonction publique fédérale et a eu des répercussions sur sa capacité de défendre ses réseaux et ses systèmes contre les cyberattaques et les personnes malveillantes qui cherchent à perturber les opérations du gouvernement.

À propos de l’audit

Le présent rapport de certification indépendant sur la cybersécurité des réseaux et des systèmes a été préparé par le Bureau du vérificateur général du Canada. Notre responsabilité était de donner de l’information, une assurance et des avis objectifs au Parlement en vue de l’aider à examiner soigneusement la gestion que fait le gouvernement des ressources et des programmes, et d’exprimer une conclusion quant à la conformité du Secrétariat du Conseil du Trésor du Canada, du Centre de la sécurité des télécommunications Canada et de Services partagés Canada, dans tous ses aspects importants, aux critères applicables.

Tous les travaux effectués dans le cadre du présent audit ont été réalisés à un niveau d’assurance raisonnable conformément à la Norme canadienne de missions de certification (NCMC) 3001 — Missions d’appréciation directe de Comptables professionnels agréés du Canada (CPA Canada), qui est présentée dans le Manuel de CPA Canada — Certification.

Le Bureau du vérificateur général du Canada (BVG) applique la Norme canadienne de gestion de la qualité (NCGQ) 1, Gestion de la qualité par les cabinets qui réalisent des audits ou des examens d’états financiers, ou d’autres missions de certification ou de services connexes. Cette norme exige que le BVG conçoive, mette en place et fasse fonctionner un système de gestion de la qualité qui comprend des politiques ou des procédures conformes aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables.

Lors de la réalisation de nos travaux d’audit, nous avons respecté les règles sur l’indépendance et les autres règles de déontologie définies dans les codes de déontologie pertinents applicables à l’exercice de l’expertise comptable au Canada, qui reposent sur les principes fondamentaux d’intégrité, d’objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Conformément à notre processus d’audit habituel, nous avons obtenu ce qui suit de la direction de chacune des entités :

- la confirmation de sa responsabilité à l’égard de l’objet considéré;
- la confirmation que les critères étaient valables pour la mission;
- la confirmation qu’elle nous a fourni tous les renseignements dont elle a connaissance et qui lui ont été demandés ou qui pourraient avoir une incidence importante sur les constatations ou la conclusion contenues dans le présent rapport;
- la confirmation que les faits présentés dans le rapport sont exacts.

Objectif de l’audit

L’objectif de l’audit consistait à déterminer si le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des télécommunications Canada et Services partagés Canada disposaient des outils nécessaires pour protéger et défendre de façon coordonnée les réseaux et les systèmes du gouvernement contre les cyberattaques.

Étendue et méthode

Dans le cadre de nos travaux d'audit, nous avons entre autres examiné des plans, des stratégies, des politiques et des lignes directrices; rencontré en entretien des représentantes et représentants des ministères et organismes pertinents; passé en revue des événements de cybersécurité antérieurs; et analysé l'adoption des services de cybersécurité clés offerts aux organisations fédérales :

- Nous avons établi l'existence et évalué la qualité des stratégies et des plans visant à répondre aux besoins du gouvernement en matière de cybersécurité, y compris ses objectifs et ses initiatives axés sur l'amélioration de sa cybersécurité.
- Nous avons obtenu une liste des organisations fédérales et avons validé cette information auprès du Secrétariat du Conseil du Trésor du Canada dans le but d'en arriver à un nombre total d'organisations fédérales. Cela représentait en tout 204 organisations fédérales : 85 organisations tenues de recourir aux services de cybersécurité des organisations auditées, 44 sociétés d'État, 9 mandataires et 66 autres organisations telles que des petits ministères et organismes, des conseils, des commissions et des tribunaux administratifs. Nous avons déterminé le nombre d'organisations fédérales qui avaient adopté les services de défense de cybersécurité visés par notre audit.
- Nous avons obtenu une liste des événements de cybersécurité et des cyberattaques ayant touché des organisations fédérales qui ont été identifiés par le Centre de la sécurité des télécommunications Canada ou qui ont été signalés à celui-ci et qui se sont produits entre les années civiles 2022 et 2024 (jusqu'à la fin de notre période d'audit). Après avoir validé la liste de cyberattaques auprès du Secrétariat du Conseil du Trésor du Canada, nous avons examiné les rapports post-événements concernant huit cyberattaques antérieures qui ont entraîné la compromission de renseignements, qui ont touché plus d'une organisation fédérale ou dont la résolution a nécessité l'intervention des entités auditées. Les exemples sélectionnés ne visaient pas à être représentatifs sur le plan statistique. Dans le cas d'une de ces cyberattaques, nous avons réalisé des travaux supplémentaires auprès de l'organisation fédérale touchée afin de mieux comprendre les détails de l'attaque, le rôle joué par l'organisation et comment celle-ci et d'autres organisations auditées ont collaboré pour intervenir en réponse à l'attaque.
- Nous avons sélectionné trois projets ou initiatives de cybersécurité en cours, à partir d'une liste combinée de 18 projets et initiatives fournie par Services partagés Canada et le Centre de la sécurité des télécommunications Canada, et évalué les progrès de leur mise en œuvre. Nous avons sélectionné ces projets et initiatives en fonction de leur valeur en dollars (budgets), des délais prévus pour leur mise en œuvre, de leur application pangouvernementale et de leur pertinence pour ce qui est de l'objectif et de l'étendue de notre audit.

En vue d'obtenir différents points de vue quant à la raison pour laquelle les sociétés d'État et les petits ministères et organismes qui n'étaient pas tenus de recourir aux services de cybersécurité des organisations auditées avaient adopté ou non les services fournis par Services partagés Canada ou les capteurs de défense de cybersécurité du Centre de la sécurité des télécommunications Canada, nous avons eu recours à un questionnaire pour interroger des représentantes et représentants et avons consulté 13 de ces organisations fédérales, 5 petits ministères et organismes et 8 sociétés d'État. Même si leurs commentaires

nous ont fourni des renseignements fort utiles, il convient de noter que la sélection de ces organisations fédérales ne visait pas à être représentative sur le plan statistique. Bien que nous ayons conscience que les points de vue exprimés peuvent correspondre à ceux d'autres organisations fédérales, nous n'avons pas validé cette hypothèse au moyen de consultations ou d'analyses supplémentaires. Les consultations avaient pour but de mieux comprendre les raisons justifiant les décisions ainsi que les défis associés à l'adoption ou non des services de cybersécurité du gouvernement.

Nous n'avons réalisé aucun test d'intrusion ni aucune autre évaluation pour tester l'efficacité des services de cybersécurité du Centre de la sécurité des télécommunications Canada ou de Services partagés Canada.

Critères

Pour tirer une conclusion par rapport à l'objectif de notre audit, nous avons utilisé les critères suivants :

Critères	Sources
Le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada, le Centre de la sécurité des télécommunications Canada et certains ministères élaborent et appliquent une approche coordonnée axée sur la collaboration afin de protéger et de défendre les réseaux et systèmes du gouvernement. Le Secrétariat du Conseil du Trésor du Canada élabore une stratégie de cybersécurité qui énonce une vision et des objectifs stratégiques afin d'améliorer la cybersécurité des opérations du gouvernement. Le Secrétariat du Conseil du Trésor du Canada définit une orientation et établit des priorités pour sécuriser les réseaux et systèmes de technologie de l'information du gouvernement. Le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada et le Centre de la sécurité des télécommunications Canada disposent de la structure de gouvernance, de l'information et des outils nécessaires pour collaborer et intervenir en cas d'événements et d'incidents de cybersécurité et produire des rapports connexes. Le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada et le Centre de la sécurité des télécommunications Canada mesurent les résultats de la posture de cybersécurité du gouvernement, y compris l'efficacité avec laquelle celui-ci réagit aux menaces.	• Loi sur le Centre de la sécurité des télécommunications • Loi sur Services partagés Canada • Conseil du Trésor, Politique sur la sécurité du gouvernement, 2019 • Conseil du Trésor, Directive sur la gestion de la sécurité, 2019 • Conseil du Trésor, Politique sur les services et le numérique, 2020 • Conseil du Trésor, Directive sur les services et le numérique, 2020 • Secrétariat du Conseil du Trésor du Canada, Ligne directrice sur les services et le numérique, 2020 • Conseil du Trésor, Politique sur les résultats, 2016 • Secrétariat du Conseil du Trésor du Canada, Plan ministériel 2024-2025 • Secrétariat du Conseil du Trésor du Canada, Stratégie intégrée de cybersécurité du gouvernement du Canada, 2024 • Secrétariat du Conseil du Trésor du Canada, Plan stratégique des opérations numériques : de 2021 à 2024 • Gouvernement du Canada, Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage, 2016

Critères	Sources
Services partagés Canada et le Centre de la sécurité des télécommunications Canada protègent les réseaux et les systèmes du gouvernement. Services partagés Canada et le Centre de la sécurité des télécommunications Canada s'acquittent de leurs responsabilités respectives de défendre et de protéger les réseaux et les systèmes du gouvernement contre les menaces et les événements de cybersécurité. Services partagés Canada et le Centre de la sécurité des télécommunications Canada cernent l'ensemble des infrastructures et des systèmes de technologie de l'information qui posent un risque et qui présentent une menace pour la cybersécurité du gouvernement fédéral. Services partagés Canada et le Centre de la sécurité des télécommunications Canada mesurent l'efficacité de leurs services de cyberdéfense. Services partagés Canada et le Centre de la sécurité des télécommunications Canada font des progrès relativement à leurs projets et initiatives de cybersécurité qui ont une incidence sur la posture générale de toutes les organisations fédérales en matière de cyberdéfense.	• Gouvernement du Canada, Renforcement de la cybersécurité au gouvernement du Canada : Avis de mise œuvre de la Politique sur la sécurité, 2024 • Services partagés Canada, Plan ministériel 2024-2025 • Services partagés Canada, Services partagés Canada 3.0 : Une approche d'entreprise • Services partagés Canada, Réaliser des solutions numériques ensemble pour le Canada • Services partagés Canada, Stratégie en matière de réseau et de sécurité, 2021 • Gouvernement du Canada, Ambition numérique du Canada 2022-2023 • Gouvernement du Canada, Ambition numérique du Canada 2023-2024 • Budgets fédéraux, 2018, 2019, 2021, 2022, 2023 et 2024 • Loi sur la gestion des finances publiques • Secrétariat du Conseil du Trésor du Canada, Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité nº 2017-01 • Secrétariat du Conseil du Trésor du Canada, Guide sur la consignation d'événements, 2020 • Secrétariat du Conseil du Trésor du Canada, Orientation sur la gestion des rustines, 2020 • Secrétariat du Conseil du Trésor du Canada, Plan de gestion des événements de cybersécurité du gouvernement du Canada, 2023 • Secrétariat du Conseil du Trésor du Canada, Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage du gouvernement du Canada • Secrétariat du Conseil du Trésor du Canada, Guide de sécurité pour les solutions de système d'information • Sécurité publique Canada, Stratégie nationale de cybersécurité, 2022 • Services partagés Canada, Feuille de route des services de cybersécurité

Critères	Sources
	• Centre canadien pour la cybersécurité, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) • Centre canadien pour la cybersécurité, 10 meilleures mesures de sécurité des TI • ISACA, Cadre COBIT 2019 : Objectifs de gouvernance et de gestion • Organisation internationale de normalisation et Commission électrotechnique internationale, ISO/IEC 27001:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences • Organisation internationale de normalisation et Commission électrotechnique internationale, ISO/IEC 27002:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information • Organisation internationale de normalisation et Commission électrotechnique internationale, ISO IEC 27004:2016, Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation (indisponible en français) • Organisation internationale de normalisation et Commission électrotechnique internationale, ISO/IEC 27005:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information • Organisation internationale de normalisation et Commission électrotechnique internationale, ISO/IEC 27010:2015, Technologies de l'information — Techniques de sécurité — Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles (indisponible en français) • Organisation internationale de normalisation et Commission électrotechnique internationale, ISO/IEC 27031:2011, Technologies de l'information — Techniques de sécurité — Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité

Critères	Sources
	• Organisation internationale de normalisation et Commission électrotechnique internationale, ISO/IEC 27032:2023, Cybersécurité — Lignes directrices relatives à la sécurité sur l'internet (indisponible en français) • Institut des auditeurs internes, Global Technology Audit Guide (GTAG): Auditing IT Governance (en anglais seulement) • Institut des auditeurs internes, Global Technology Audit Guide (GTAG): Assessing Cybersecurity Risk (en anglais seulement) • Institut des auditeurs internes, Global Technology Audit Guide (GTAG): Auditing Cyber Incident Response and Recovery, 2022 (en anglais seulement) • Agence de l'Union européenne pour la cybersécurité, Good Practices for Security of IoT: Secure Software Development Lifecycle (en anglais seulement) • National Institute of Standards and Technology, NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations (ébauche, en anglais seulement), 2017 • National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (en anglais seulement), 2018 • National Institute of Standards and Technology, NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (en anglais seulement), 2018 • National Institute of Standards and Technology, NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments (en anglais seulement), 2012 • Project Management Institute, Guide du corpus des connaissances en management de projet (Guide PMBOK), 7e édition, 2021 • Nations Unies, Transformer notre monde : le Programme de développement durable à l'horizon 2030, 2015

Période visée par l’audit

L’audit a porté sur la période allant du 1er octobre 2023 au 30 septembre 2024. Il s’agit de la période à laquelle s’applique la conclusion de l’audit. Toutefois, afin de mieux comprendre l’objet considéré de l’audit, nous avons aussi examiné certains dossiers antérieurs à cette période.

Date du rapport

Nous avons fini de rassembler les éléments probants suffisants et appropriés à partir desquels nous avons fondé notre conclusion le 22 septembre 2025, à Ottawa, au Canada.

Équipe d’audit

L’audit a été réalisé par une équipe multidisciplinaire du Bureau du vérificateur général du Canada (BVG) dirigée par Jean Goulet, directeur principal. Le directeur principal est responsable de la qualité de l’audit dans son ensemble; il doit s’assurer notamment que les travaux d’audit sont exécutés conformément aux normes professionnelles, aux exigences des textes légaux et réglementaires applicables ainsi qu’aux politiques et au système de gestion de la qualité du BVG.

Recommandations et réponses

Les réponses figurent telles qu'elles ont été reçues par le Bureau du vérificateur général du Canada.

Dans ce tableau, le numéro du paragraphe qui précède la recommandation indique l'emplacement de la recommandation dans le rapport.

Recommandation	Réponse
25. Services partagés Canada, en collaboration avec le Centre de la sécurité des télécommunications Canada, devrait établir un plan d'action clair comprenant des critères définis et un échéancier pour mettre au point une application de gestion de l'information et des événements de sécurité qui corrige les lacunes existantes en matière de surveillance de la cybersécurité	**Réponse du Ministère** — Recommandation acceptée. Nous sommes d'accord avec la recommandation. Services partagés Canada (SPC) a recommencé le travail visant le projet de gestion des informations et des événements de sécurité (GIES) et s'engage à mener à bien le projet. Une fois le projet achevé, cela permettra d'avoir une connaissance de la situation plus efficacement dans l'ensemble des environnements du gouvernement du Canada (GC). Le Ministère s'efforce actuellement de terminer le processus d'approvisionnement en cours et demandera qu'on lui accorde les pouvoirs de passation de marchés nécessaires d'ici décembre 2025. SPC intensifiera sa collaboration en cours avec le Centre de la sécurité des télécommunications (CST) pour trouver des accords qui facilitent la conclusion d'ententes de financement appropriées pour l'analyse des événements quotidiens touchant le périmètre de cybersécurité d'ici à ce que le projet de GIES soit terminé.
30. Services partagés Canada devrait : • s'assurer de disposer d'un inventaire central à jour des réseaux et des systèmes qu'il dessert dans l'ensemble des organisations fédérales, ainsi que d'un processus pour gérer les appareils qui ont besoin de correctifs, de mises à jour ou d'entretien, ou qui doivent être remplacés. Le Ministère devrait installer les correctifs requis, apporter les mises à jour nécessaires et assurer l'entretien et le remplacement des réseaux et des systèmes en conséquence; • déterminer une solution aux difficultés auxquelles se heurte le projet Visibilité, sensibilisation et sécurité de point d'extrémité.	**Réponse du Ministère** — Recommandation acceptée. Nous sommes d'accord avec la recommandation. En 2024, SPC a entamé une initiative de transformation de la gestion du matériel dans le but de renforcer ses processus et ses systèmes de gestion des actifs. Cette initiative devrait continuer de permettre des améliorations progressives aux mesures de contrôle du cycle de vie des biens de SPC jusqu'à ce qu'elles soient toutes apportées en mars 2028. Le Ministère s'engage à régler les difficultés rencontrées dans le cadre du projet de visibilité, sensibilisation et sécurité de point d'extrémité. Un contrat devrait être octroyé d'ici la fin de 2025.

Recommandation	Réponse
31. Le Secrétariat du Conseil du Trésor du Canada, en consultation avec le Centre de la sécurité des télécommunications Canada, devrait s'assurer que les organisations fédérales : • installent des capteurs de défense de cybersécurité sur tous ses points d'extrémité afin de repérer les vulnérabilités; • corrigent rapidement les vulnérabilités.	**Réponse du Secrétariat** — Recommandation acceptée. Le Secrétariat du Conseil du Trésor du Canada (SCT), en consultation avec le Centre de la sécurité des télécommunications Canada (CST), collaborera avec les organisations fédérales afin de veiller à ce que des capteurs de cyberdéfense soient mis en place sur tous les points d'extrémité, de manière que leurs vulnérabilités puissent être identifiées et corrigées en temps opportun. Cela comprend l'exploitation de la capacité de visibilité et sécurité des points d'extrémité (VSPE) qui sera disponible dans le cadre de l'initiative Visibilité, sensibilisation et sécurité de point d'extrémité (VSSPE) du Services partagés Canada (SPC), qui permettra au Gouvernement du Canada (GC) d'identifier les actifs sur lesquels aucun capteur de cyberdéfense n'est déployé. De plus, conformément au Plan de mise en œuvre de la Stratégie intégrée de cybersécurité du GC, la création d'un inventaire fédéré des applications et des systèmes du GC permettra de rationaliser la collecte et la mise à jour des actifs applicatifs du GC. En outre, dans le cadre du Programme de gestion des vulnérabilités d'entreprise du GC, le SCT, en collaboration avec le SPC et le CCCS, travaillera avec les ministères pour identifier, évaluer et classer par ordre des priorités la correction des vulnérabilités des points d'extrémité selon une approche fondée sur les risques. Lors de sa prochaine occasion cyclique, le SCT cherchera à obtenir un financement continu pour soutenir ces initiatives.

Recommandation	Réponse
35. Le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des télécommunications Canada et Services partagés Canada devraient réévaluer leurs pratiques de gestion des incidents de cybersécurité pour améliorer la coordination et favoriser la communication rapide de l'information essentielle requise pour intervenir lors de cyberattaques visant des organisations fédérales.	**Réponse des trois entités** — Recommandation acceptée. Le Secrétariat du Conseil du Trésor du Canada (SCT), le Centre de la sécurité des télécommunications Canada (CST) et Services partagés Canada (SPC) réévalueront leurs pratiques et protocoles de gestion des incidents de cybersécurité afin de permettre une meilleure coordination et un partage rapide des informations critiques nécessaires lors de la réponse aux cyberattaques touchant les organisations fédérales. Cela comprend la mise à l'essai du Plan de gestion des événements de cybersécurité du GC (PGEC GC) au moyen d'un exercice de simulation de cybersécurité afin d'en assurer l'efficacité. Par la suite à l'exercice de simulation de cybersécurité, le SCT mettra à jour et publiera le PGEC GC au plus tard à la fin de l'exercice 2025-2026. De plus, conformément au Plan de mise en œuvre de la Stratégie intégrée de cybersécurité du GC, la création d'une plateforme de collaboration pour les événements de cybersécurité et d'un outil de gestion des incidents de cybersécurité à l'échelle du GC permettra une collaboration harmonieuse dans la gestion de la réponse du GC aux évènements cybernétiques. Cela comprend le soutien d'un partage centralisé de l'information et du suivi des mesures d'atténuation internes du GC lors d'un événement de cybersécurité du GC, tant pour les organismes centraux que pour les organisations du GC. Le SCT et SPC appuieront le CST, qui est responsable de l'élaboration et de la mise en œuvre d'une plateforme et d'un outil de gestion des événements de cybersécurité.

Recommandation	Réponse
36. Le Centre de la sécurité des télécommunications Canada devrait parachever sa demande de financement et prioriser ses travaux d'élaboration et de mise en œuvre d'une plateforme de collaboration en matière d'événements de cybersécurité et d'un outil de gestion des incidents. La nouvelle plateforme et le nouvel outil devraient permettre de normaliser la communication, le suivi, la surveillance et la consignation des événements de cybersécurité; le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada et d'autres organisations fédérales devraient pouvoir y accéder.	**Réponse de l'organisme** — Recommandation acceptée. Le Centre de la sécurité des télécommunications Canada demandera du financement pour la création d'une plateforme de collaboration lors d'événements de cybersécurité à l'échelle du GC et d'un outil de gestion des cas d'incidents afin de permettre une collaboration transparente lors de la gestion de la réponse du GC aux cyber événements. Cela comprend le soutien au partage centralisé d'informations et au suivi des efforts internes d'atténuation du GC lors d'un événement de cybersécurité du GC pour les agences centrales et les organisations du GC. Achèvement prévu : Inconnu, sous réserve de la décision du gouvernement.

Annexe — Descriptions textuelles des pièces

Voici les descriptions textuelles des pièces.

Pièce 1 — Événement de cybersécurité, incident de cybersécurité et cyberattaque — Description textuelle

Ce graphique définit les termes « événement de cybersécurité », « incident de cybersécurité » et « cyberattaque » et donne des exemples pour chacun. Il montre également qu'un événement de cybersécurité comprend un incident de cybersécurité et qu'un incident de cybersécurité comprend une cyberattaque.

Dans un système ou un réseau, un incident de cybersécurité est défini comme tout événement ou changement observable susceptible d'être pertinent sur le plan de la sécurité. Les événements ne sont pas forcément synonymes d'atteinte à la sécurité ou de violation, mais peuvent devenir des incidents.Voici deux exemples d'événements de cybersécurité :

- utilisatrice ou utilisateur qui se connecte à un système à une heure inhabituelle;
- pare-feu qui bloque une connexion.

Un incident de cybersécurité est un événement non autorisé ou perturbateur qui nuit aux systèmes informatiques, aux réseaux ou aux données. Il comprend les événements intentionnels (malveillants) et non intentionnels (accidentels). Les incidents de cybersécurité sont tous des événements, mais ne sont pas tous des attaques. Voici deux exemples d'incidents de cybersécurité :

- accès non autorisé à un système;
- divulgation accidentelle de données.

Une cyberattaque est un acte délibéré et malveillant visant à accéder à des systèmes informatiques, à des réseaux ou à des appareils, à y créer des perturbations ou des dommages ou à y voler de l'information. Toutes les cyberattaques constituent des incidents de cybersécurité. Voici trois exemples de cyberattaques :

- attaque par rançongiciel;
- attaque par déni de service;
- vol de données.

Source : D'après des renseignements du Centre de la sécurité des télécommunications Canada et du Secrétariat du Conseil du Trésor du Canada

Retour à la pièce 1

Pièce 2 — Objectifs et mesures clés de la Stratégie intégrée de cybersécurité du gouvernement du Canada — Description textuelle

Ce graphique présente les objectifs et des exemples de mesures clés de la Stratégie intégrée de cybersécurité du gouvernement du Canada.

La vision de la stratégie est la suivante : « Construire un gouvernement fédéral de classe mondiale, durable et résilient pour réduire les risques liés à la cybersécurité afin que les ministères et les organismes puissent fournir des services numériques sûrs et fiables ». Les organisations fédérales responsables de la mise en œuvre de la stratégie sont le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des télécommunications Canada, Services partagés Canada et d'autres ministères et organismes.

Le graphique présente quatre objectifs de la stratégie et deux exemples de mesures clés pour chaque objectif. La stratégie comporte de nombreuses autres mesures. Les exemples énoncés ici représentent une partie des mesures ayant une portée pangouvernementale.

- Objectif de la stratégie : Expliquer clairement les risques liés à la cybersécurité et leur incidence sur les opérations. Les deux exemples de mesures clés sont les suivants :
    - établir un programme pangouvernemental de conformité et d'assurance pour évaluer les mécanismes de défense ministériels en matière de cybersécurité afin de cerner les risques de cybersécurité et d'en établir les priorités;
    - créer un programme pangouvernemental de gestion des vulnérabilités afin de gérer et de réduire les vulnérabilités qui touchent les systèmes et les réseaux du gouvernement.
- Objectif de la stratégie : Prévenir les cyberattaques et y résister plus efficacement. Les deux exemples de mesures clés sont les suivants :
    - déployer les mécanismes de défense en matière de cybersécurité dans les petits ministères et organismes;
    - établir un cadre permettant de mieux détecter et prévenir les activités frauduleuses visant les applications gouvernementales.
- Objectif de la stratégie : Renforcer les capacités et la résilience à l'échelle du gouvernement du Canada. Les deux exemples de mesures clés sont les suivants :
    - établir un cadre permettant aux ministères de tenir des inventaires exacts des applications et systèmes du gouvernement. Mener tout au long de l'année des essais et des examens de la protection et des mécanismes de défense en matière de cybersécurité;
    - mettre en place une plateforme pangouvernementale de collaboration concernant les événements de cybersécurité afin de gérer les événements de cybersécurité et d'y répondre.
- Objectif de la stratégie : Établir un effectif fédéral diversifié et doté des compétences nécessaires en cybersécurité. Les deux exemples de mesures clés sont les suivants :
    - développer les talents en matière de cybersécurité grâce à des programmes de formation interfonctionnelle;
    - favoriser une culture de gestion des talents afin de recruter et de retenir des candidats qualifiés.

Source : D'après des renseignements contenus dans la Stratégie intégrée de cybersécurité du gouvernement du Canada, Secrétariat du Conseil du Trésor du Canada, 2024

Retour à la pièce 2

Pièce 3 — Le Centre de la sécurité des télécommunications Canada a conçu trois types de capteurs de défense de cybersécurité pour détecter et atténuer les événements de cybersécurité et les cyberattaques — Description textuelle

Ce graphique présente les trois types de capteurs de défense de cybersécurité mis au point par le Centre de la sécurité des télécommunications, ainsi que l'année de mise en œuvre de chacun.

En 2010, le Ministère a mis en œuvre le capteur au niveau du réseau, qui détecte et atténue les incidents sur les réseaux du gouvernement. Ce capteur est habituellement intégré au service Internet d'entreprise de Services partagés Canada.

En 2012, le Ministère a mis en œuvre le capteur au niveau de l'hôte, qui détecte les cyberattaques sur les terminaux informatiques tels que les ordinateurs portables, les serveurs et les réseaux locaux. Le capteur analyse et traite l'information recueillie afin de détecter des événements de cybersécurité suspects survenant sur un appareil hôte. L'information recueillie sert à signaler les anomalies et les faiblesses aux organisations fédérales concernées.

En 2019, le Ministère a mis en œuvre le capteur infonuagique, qui fonctionne dans l'infrastructure infonuagique des organisations fédérales de pair avec les mécanismes de défense des fournisseurs de services infonuagiques. Le capteur automatise la collecte de l'activité consignée dans le nuage et analyse l'information afin de détecter et d'atténuer les événements de cybersécurité suspects.

Source : D'après des renseignements du Centre de la sécurité des télécommunications Canada

Retour à la pièce 3

Pièce 4 — Les 119 organisations fédérales qui n'étaient pas tenues de recourir aux services de cybersécurité de Services partagés Canada et du Centre de la sécurité des télécommunications Canada étaient encouragées à y recourir, mais beaucoup ont choisi de ne pas le faire — Description textuelle

Cette pièce comprend deux graphiques; le premier présente le nombre d'organisations fédérales qui ont choisi d'utiliser le service Internet d'entreprise de Services partagés Canada, et le deuxième présente le nombre d'organisations fédérales qui ont choisi d'utiliser les capteurs de défense de cybersécurité du Centre de la sécurité des télécommunications Canada.

Sur les 119 organisations fédérales qui n'étaient pas tenues de recourir au service Internet d'entreprise de Services partagés Canada, 24 organisations (soit 20 %) avaient choisi de l'utiliser volontairement, tandis que 95 (soit 80 %) ne l'utilisaient pas.

Par ailleurs, sur ces 119 organisations, 76 (soit 64 %) avaient choisi d'utiliser un ou des capteurs de défense de cybersécurité du Centre de la sécurité des télécommunications Canada, tandis que 43 (soit 36 %) ne l'avaient pas fait.

Source : D'après des données de Services partagés Canada et du Centre de la sécurité des télécommunications Canada

Retour à la pièce 4

Bureau du
vérificateur général
du Canada

Office of the
Auditor General
of Canada