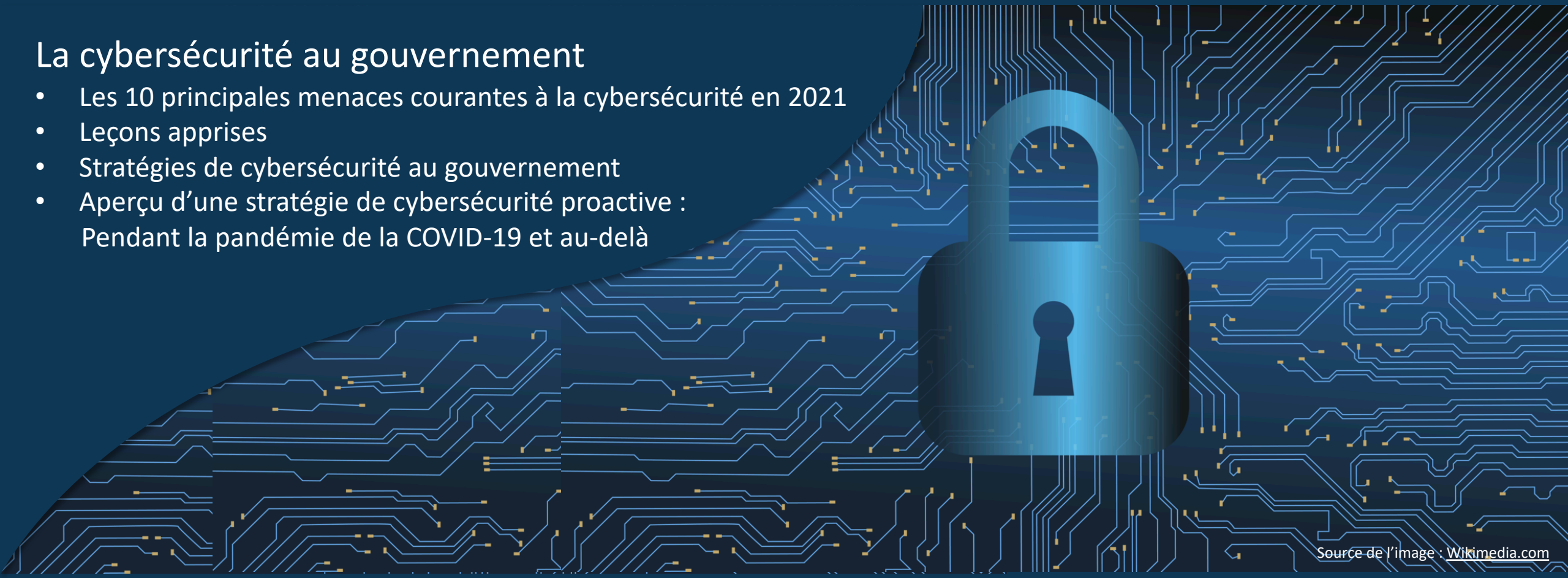
Citizen F1RST

OPTIMISÉ PAR
L'Institut des services axés sur les citoyens

La cybersécurité au gouvernement

- Les 10 principales menaces courantes à la cybersécurité en 2021
- Leçons apprises
- Stratégies de cybersécurité au gouvernement
- Aperçu d'une stratégie de cybersécurité proactive : Pendant la pandémie de la COVID-19 et au-delà



Source de l'image : Wikimedia.com

RAPPORT MENSUEL DES CONSEILS MIXTES À L'INTENTION DES CADRES

Élaboré par le Comité de recherche

Novembre 2021

1. Introduction

Selon le gouvernement du Canada, « **la cybersécurité est la protection des données numériques stockées dans votre environnement des cybermenaces contre les cybermenaces et les auteurs de cybermenace**[1] ». La pandémie de la COVID-19 (« la pandémie ») a intensifié la demande de connectivité numérique et de gouvernement numérique. Les restrictions imposées par le gouvernement en réponse à la pandémie ont mené à des environnements de travail à distance pour les employés, et les clients comptent principalement sur la prestation de services en ligne pour accéder aux services gouvernementaux. La dépendance croissante à l'égard de la connectivité numérique a accentué le besoin de services axés sur le numérique[2].

Cette évolution de plus en plus rapide vers les services numériques et en ligne a augmenté l'importance de la cybersécurité plus que jamais auparavant. Pendant la pandémie, les cyberattaques se sont multipliées dans le monde entier. Selon l'autorité canadienne en matière de cybersécurité, le Centre canadien pour la cybersécurité, les cybercriminels adaptent constamment leurs méthodes et utilisent des techniques plus avancées pour attaquer les systèmes gouvernementaux[3]. Les changements dans les habitudes de travail et d'infrastructure causés par la pandémie sont essentiellement attribuables à l'affaiblissement des mesures de cybersécurité.

Afin d'accroître les efforts en matière de cybersécurité pendant la pandémie, ainsi que dans le monde tel qu'il existera après la pandémie, il est essentiel que les gouvernements examinent leurs stratégies de cybersécurité et prennent des mesures concrètes pour promouvoir un Internet plus fiable. Ces mesures contribueront à renforcer la confiance numérique et à créer un environnement de cybersécurité solide où les clients peuvent accéder aux services gouvernementaux en ligne facilement et en toute sécurité.

Pourquoi ce rapport est-il important?

- L'amélioration de la cybersécurité est une priorité absolue pour les Canadiens. Selon le baromètre de confiance Edelman pour 2021, « 65 % des Canadiens craignent d'être victimes d'une cyberattaque, ce qui dépasse le changement climatique (63 %) et la COVID-19 (60 %)[4] ».
- Partout au Canada, des administrations ont signalé un nombre croissant de cybercriminels et d'autres groupes malveillants en ligne qui exploitent l'éclosion de la COVID-19 pour en tirer un avantage personnel[5].
- En 2020, le Comité de recherche a publié un rapport intitulé *Cybersécurité* : *Un regard sur l'environnement canadien*. Ce rapport présente des organisations et initiatives de cybersécurité au Canada, décrit les possibilités et les défis dans l'espace de cybersécurité, et détermine où les gouvernements devraient concentrer leurs efforts.

Qu'est-ce qui est couvert dans ce rapport exécutif?

Le présent rapport comprend les éléments suivants :

- Introduction
- Les 10 principales menaces courantes à la cybersécurité en 2021
- Leçons apprises
- Stratégies de cybersécurité au gouvernement
- Aperçu d'une stratégie de cybersécurité proactive : Pendant la pandémie de la COVID-19 et au-delà

1. Qu'est-ce que la cybersécurité?
2. How Covid-19 is Dramatically Changing Cybersecurity
3. Conseils ciblés sur la cybersécurité applicables durant la pandémie de la COVID-19
4. La cybersécurité préoccupe davantage les Canadiens que la COVID-19 – Voici comment le Canada peut intensifier ses efforts : La Chambre de commerce du Canada
5. Cyberrisques : Une menace accrue pendant la pandémie de la COVID-19

2. Les 10 principales menaces courantes à la cybersécurité en 2021

Pendant la pandémie, le nombre d'incidents de cybersécurité signalés au Canada a augmenté à un rythme inquiétant. Selon un nouveau rapport d'IBM Security, le coût moyen d'une atteinte à la sécurité des données au Canada était de 6,75 millions de dollars par incident au cours de l'année d'enquête 2021. Il s'agit d'une hausse par rapport à l'année 2020, alors que ce montant se chiffrait à 6,35 millions de dollars, et du montant le plus élevé depuis qu'IBM a inclus le Canada dans son enquête il y a sept ans[6]. Selon le ministère de la Sécurité publique et de la Protection civile et d'éminents chercheurs en sécurité de l'information, voici les 10 principales menaces à la cybersécurité que les organisations et les particuliers ont connues en 2021[7] :

1. **Attaques du jour zéro :** Une vulnérabilité logicielle découverte par des cyberpirates avant que le fournisseur ou l'organisation en ait pris connaissance. Les attaques du jour zéro sont de plus en plus sophistiquées et représentent une menace importante en 2021.	6. **Hameçonnage :** Un type d'attaque par fraude psychologique souvent utilisé pour voler les données de l'utilisateur, y compris les identifiants de connexion et les numéros de carte de crédit. Il s'est avéré très efficace au XXIe siècle parce qu'il est couramment utilisé par l'entremise de faux courriels, de messages textes ou de sites Web fictifs qui semblent authentiques.
2. **Internet des objets (IdO) :** Grâce à l'IdO, les capteurs recueillent, communiquent, analysent et utilisent l'information. Même si cela apporte de la valeur pour les organisations et les clients parce que l'efficacité de l'expérience est accrue, cela crée également de nouveaux risques que l'information soit compromise. Au cours de l'année 2021, il y a eu plus d'atteintes à la vie privée à partir d'appareils qui utilisent l'IdO.	7. **Rançongiciels :** Il s'agit d'un type de maliciel qui utilise le chiffrement pour conserver les renseignements d'une victime et exiger une rançon en échange. Les données essentielles d'un utilisateur ou d'une organisation sont chiffrées de façon à ce qu'il soit impossible d'accéder aux fichiers, aux bases de données ou aux applications. En 2021, les rançongiciels sont devenus une menace croissante, générant des milliards de dollars en paiements aux cybercriminels et causant des dommages et des dépenses importants aux organisations des secteurs public et privé.
3. **Réseaux de zombies :** Réseaux de dispositifs informatiques détournés utilisés pour effectuer diverses fraudes et cyberattaques. En 2021, la menace des réseaux de zombies a pris beaucoup d'ampleur en raison de la popularité des dispositifs d'automatisation de maison intelligents qui se connectent à Internet.	8. **Maliciels de minage clandestin :** Ce type de cybercriminalité consiste à infiltrer les appareils d'une personne ou d'une organisation (ordinateurs, téléphones intelligents, tablettes ou même serveurs) à son insu pour miner une cryptomonnaie. En 2021, le nombre d'attaques de minage clandestin continuent d'augmenter.
4. **Attaques par déni de service distribué (DDoS) :** Méthode utilisée par les cybercriminels pour encombrer un réseau d'un trafic malveillant de grande ampleur, ce qui nuit à la capacité de communication ou de fonctionnement normale du réseau. Cela entrave la fréquentation normale d'un site Web.	9. **Maliciels invisibles ou subversion de logiciels :** Les cyberpirates utilisent maintenant cette nouvelle forme d'attaque sophistiquée, des « maliciels invisibles », que les pare-feu ne peuvent arrêter et que les anti-maliciels ne peuvent trouver ou supprimer. Bien que ce cyberrisque en particulier puisse être considéré comme une nouvelle menace en 2021, il est en fait lié aux méthodes de piratage habituelles.
5. **Pourriels :** Bien que le Canada ait adopté une loi interdisant la distribution de messages publicitaires sans sollicitation, le pourriel est un problème mondial qui continue de s'aggraver en 2021.	10. **Attaques par interception :** Attaque qui consiste à intercepter une communication entre deux parties pour écouter secrètement ou modifier les données échangées entre elles. Les cyberpirates peuvent utiliser les attaques par interception pour voler des justificatifs d'identité ou des renseignements personnels, espionner la victime, saboter les communications ou corrompre les données.

6. Cost of data breaches in Canada hit new record in 2021: IBM
7. Common Cybersecurity Threats

3. Leçons apprises pendant la pandémie de la COVID-19

La pandémie a révélé qu'il est essentiel de se préparer pour réussir à limiter les risques liés aux cyberattaques. La capacité des organisations de réagir rapidement à des événements imprévus aide à réduire l'incidence d'une cyberattaque.

Pour le gouvernement, la question ne doit pas être de savoir ***si*** une attaque surviendra, mais ***à quel moment***, et il doit reconnaître que les conséquences des rançongiciels et des atteintes à la confidentialité des données peuvent avoir des répercussions financières négatives[8]. Il est également important d'être conscient que le gain financier n'est pas le seul motif des cyberattaques. Le cyberactivisme et son objectif de nuire à la réputation des organisations gouvernementales constituent une menace supplémentaire[9].

Tout au long de la pandémie, plusieurs incidents de cybersécurité ont été signalés dans les administrations canadiennes. Selon le Forum économique mondial, voici quelques-unes des principales leçons apprises pendant la pandémie[10] :

Favoriser une culture de cyberrésilience

Pour être résilient, il faut que les plus hauts niveaux de la direction reconnaissent l'importance de la gestion proactive des risques et qu'ils mettent davantage l'accent sur la capacité de l'organisation d'amortir une cyberattaque qui perturberait les services essentiels et de s'en rétablir.

Mettre l'accent sur la protection des biens et des services essentiels

Les organisations doivent avoir une vision globale et systémique de leurs services, applications, fournisseurs et biens essentiels. Les dirigeants doivent déterminer les ressources et les investissements prioritaires dans les domaines les plus importants afin de maintenir la continuité opérationnelle, protéger les biens numériques critiques et assurer la conformité.

Concilier les décisions fondées sur le risque pendant la crise et au-delà

La gestion des cyberrisques doit être revue de fond en comble. Les indicateurs classiques de cyberrésilience se sont révélées être une représentation inadéquate du risque réel. Les organisations doivent revoir leur approche à l'égard des chaînes d'approvisionnement, définir des indicateurs pratiques et judicieux des cyberrisques et miser sur les risques pour les opérations lorsqu'elles conçoivent de nouvelles stratégies relatives au numérique.

Mettre à jour et à l'essai les plans d'intervention et de continuité des activités

La crise de la COVID-19 a fait ressortir l'importance d'adapter et de mettre à l'essai régulièrement les plans d'intervention et de résilience dans les pires scénarios (y compris les pandémies) avec les principaux fournisseurs et partenaires commerciaux. Il s'agit notamment de faire en sorte que les équipes de gestion acquièrent les compétences et l'expérience nécessaires pour être en mesure de gérer la situation lorsque la pression est forte.

Renforcer la collaboration à l'échelle de l'écosystème

Le partenariat et la collaboration en matière de cyberrésilience entre le secteur public et le secteur privé dans l'ensemble de l'écosystème sont essentiels. Cela favorisera un échange d'information transparent et une sensibilisation concertée, et les secteurs pourront travailler ensemble pour perturber les activités criminelles en créant une approche systémique de la gestion du risque dans l'ensemble de la collectivité.

8, 9. Impact de la COVID-19 sur la cybersécurité
10. Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic

4. Stratégies de cybersécurité au gouvernement

Tandis que les cyberpirates continuent d'inventer de nouvelles façons de contourner les mesures de sécurité pour voler, exposer ou détruire des données de nature délicate pour des gains financiers, les organisations gouvernementales sont des cibles particulièrement vulnérables comparativement à d'autres industries. Selon Mckinsey, les gouvernements (tous les ordres) sont plus susceptibles de subir une cyberattaque pour les raisons suivantes[11] :

1. Les organisations gouvernementales hébergent des renseignements et des données sur les clients de nature très délicate.
2. La transition rapide vers le travail à domicile en réponse à la pandémie. Les employés qui travaillent à distance courent un plus grand risque que ceux qui travaillent au bureau. Cela s'explique principalement par le fait que les connexions à domicile sont généralement moins sécurisées, ce qui permet aux cybercriminels d'accéder plus facilement au réseau de l'organisation.
3. Le manque de professionnels de la cybersécurité pour répondre à la demande croissante de solutions proactives aux cyberrisques.

La cybersécurité est une priorité clé dans l'ensemble des administrations canadiennes. Voici quelques exemples de stratégies de cybersécurité au Canada.

11. Cybersecurity's dual mission during the coronavirus crisis
12. Plan d'action national en matière de cybersécurité (2019-2024)
13. Gouvernement de l'Alberta : Stratégie de cybersécurité
14. Gouvernement de la Colombie-Britannique : Politique sur la sécurité de l'information, V4.0
15. L'Ontario nomme un nouveau Comité d'experts pour la cybersécurité

Exemples de stratégies de cybersécurité dans l'ensemble du secteur public canadien

Gouvernement du Canada

La Stratégie nationale de cybersécurité décrit le cadre qui aide le gouvernement du Canada à protéger les clients contre les cybermenaces et à tirer parti des possibilités économiques offertes par la technologie numérique[12]. Cette stratégie vise à favoriser l'adaptation du gouvernement afin qu'il atteigne ses objectifs à mesure que les technologies et les cybermenaces évoluent.

Alberta

La stratégie de cybersécurité du gouvernement de l'Alberta, intitulée *Protecting the Province's Digital Assets* [protéger les biens numériques de la province], décrit les cybermenaces qui peuvent avoir une incidence sur le gouvernement de l'Alberta. Le document met également en évidence des stratégies et des principes généraux qui visent à définir, à évaluer et à prévenir ces menaces afin d'y réagir pour protéger les biens technologiques et les ressources d'information de l'organisation ou de récupérer ces biens advenant une catastrophe[13].

Colombie-Britannique

Le document intitulé *Information Security Policy* [politique sur la sécurité de l'information] décrit l'approche ministérielle du gouvernement en matière de gestion de la sécurité de l'information. Tous les ministères utilisent ce cadre pour veiller à ce que les pratiques du gouvernement en matière de sécurité de l'information soient raisonnables, appropriées et efficaces. Le document vise à protéger les renseignements personnels et confidentiels des clients d'une manière conforme aux exigences de sécurité de la *Loi sur l'accès à l'information et la protection de la vie privée* et de la *Loi sur la gestion de l'information*[14].

Ontario

La stratégie de cybersécurité de l'Ontario établit le cadre de modernisation du programme de cybersécurité de l'Ontario en mettant l'accent sur trois domaines : L'amélioration de la collaboration entre le gouvernement et le secteur parapublic; la sécurité continue des applications gouvernementales et la protection des données de nature délicate des clients. Dans le cadre de la Stratégie, le gouvernement a nommé dix membres à un comité d'experts pour aider à moderniser la cybersécurité dans l'ensemble du secteur public de l'Ontario. Le comité d'experts présentera à l'automne 2022 un rapport définitif qui contiendra des conclusions et des recommandations sur les vulnérabilités communes[15].

5. Aperçu d'une stratégie de cybersécurité proactive : Pendant la pandémie de la COVID-19 et au-delà

En réponse à la pandémie de la COVID-19, les organisations gouvernementales du Canada ont accéléré l'investissement dans la transformation numérique afin de maintenir la continuité des activités et de répondre aux besoins des clients. Bon nombre des programmes et des services ont accéléré la planification et l'élaboration de projets; ce qui devait prendre des années a duré quelques mois[16]. Cela a accru l'exposition et la vulnérabilité du gouvernement aux cybermenaces.

Dans le contexte où la pandémie évolue et modifie le fonctionnement des systèmes socioéconomiques, les cybercriminels poursuivront leurs efforts pour exploiter les failles numériques. Pour demeurer vigilants et efficaces, les gouvernements (tous les ordres) auront besoin de nouvelles approches pour relever les défis croissants en matière de cybersécurité[17]. Tout comme la technologie, la cybersécurité devra également mettre l'accent sur le renforcement et l'accroissement de la résilience organisationnelle à l'avenir.

Selon PwC, les cinq points suivants sont essentiels à l'élaboration d'une stratégie de cybersécurité proactive qui répond aux demandes changeantes pendant la pandémie et au-delà.

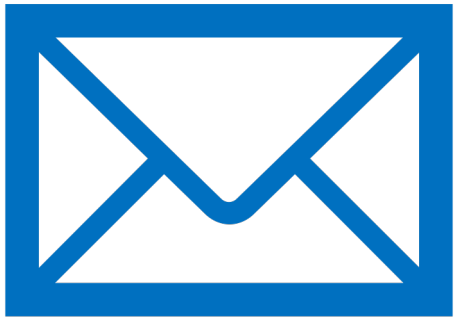
Ressources pour appuyer vos efforts en matière de cybersécurité

- Conseils ciblés sur la cybersécurité applicables durant la pandémie de la COVID-19
- L'incidence continue de la COVID-19 sur les activités de cybermenaces
- Rançongiciels : Comment les prévenir et s'en remettre
- Élaborer un plan d'intervention en cas d'incident

16, 17. Follow the leaders: How governments can combat intensifying cybersecurity risks
18. Perspectives canadiennes du sondage Global Digital Trust 2021 : La cybersécurité arrive à maturité

Aperçu d'une stratégie de cybersécurité proactive : Pendant la pandémie de la COVID-19 et au-delà[18]

Redéfinir votre stratégie de cybersécurité	• Redéfinissez votre stratégie de cybersécurité pour vous adapter à la nouvelle réalité opérationnelle et rendre la très grande vitesse du changement numérique plus sécuritaire. • Envisagez une stratégie de cybersécurité axée sur les activités qui s'harmonise avec la vision et les objectifs de l'ensemble de l'organisation et non seulement avec la TI.
Repenser votre budget de cybersécurité	• Repensez le processus de budgétisation de la cybersécurité de l'organisation pour montrer clairement comment les dépenses dans ce domaine sont liées aux risques et aux priorités opérationnels. • Liez le budget de cybersécurité aux budgets globaux de numérisation et d'automatisation. • Quantifiez les cyberrisques pour permettre à l'organisation d'évaluer les répercussions de chaque projet de cybersécurité.
Uniformiser les règles du jeu avec les cyberpirates	• Explorez des façons novatrices de protéger le nuage de l'organisation en tirant pleinement parti des capacités du nuage. Cela permettra de réduire les coûts de gouvernance, de s'attaquer proactivement aux menaces émergentes et de se conformer continuellement aux exigences. • Réinventez la façon de protéger les systèmes industriels et IdO, pour lesquels les méthodes classiques de sécurité de la TI sont inefficaces. • À mesure qu'elles sont diffusées, intégrez les pratiques de l'organisation en matière de protection de la vie privée, de protection des données et de gouvernance des données afin d'inspirer confiance dans l'utilisation des données essentielles.
Renforcer la résilience pour n'importe quel scénario	• Effectuez régulièrement des évaluations et des tests pour déceler les points faibles des moyens de défense de l'organisation avant que les cyberpirates ne le fassent. • Mettez en œuvre un programme de cyberhygiène pour remédier aux faiblesses souvent exploitées par les cyberpirates. • Mettez l'accent sur la confiance numérique à l'échelle de l'organisation en coordonnant les efforts de résilience dans les domaines de la continuité des activités, de la reprise après sinistre, de la gestion des crises, de la protection des renseignements personnels et de la fraude.
Assurer l'avenir de l'équipe de sécurité	• Concevez des programmes d'attraction et de rétention des talents pour la fonction de cybersécurité. • Offrez du perfectionnement pour accroître l'expertise des employés actuels. • Créez une formation adaptée sur la cybersécurité pour aider les employés à éviter les incidents de cybersécurité et à renforcer la culture globale de cybersécurité.



Lectures suggérées

- Three things Canada can do to become a cybersecurity leader
- 5 cybersecurity issues that the public sector faces and how to protect it
- Cities employed new cybersecurity strategies during the pandemic
- 9 notable government cybersecurity initiatives of 2021
- Canada's fledgling cybersecurity centre must do more collaborating and educating

Autres articles dignes de mention

Critical considerations for moving to the cloud

Governments look to digital ID for modern services and economic growth

The Evolution Of Voice In Elevating The User Experience

How to Address Growing Security and Privacy Challenges

How robotic process and intelligent automation are altering government performance

Ressources de recherche

Accédez aux Ressources de recherche de Citoyens en tête.

Entrées récentes dans les Ressources de recherche :

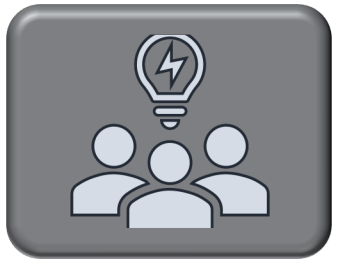
Confiance et identité numériques : Répondre aux nouvelles attentes en matière de prestation de services publics – rapport des conseils mixtes à l'intention des cadres d'octobre 2021

Le présent rapport traite des éléments suivants : l'adoption de l'identité numérique par le gouvernement, les services d'ouverture de séance comme point de départ, les justificatifs d'identité numériques vérifiables pour divers types de données et les recommandations pour faire progresser la mise en œuvre.

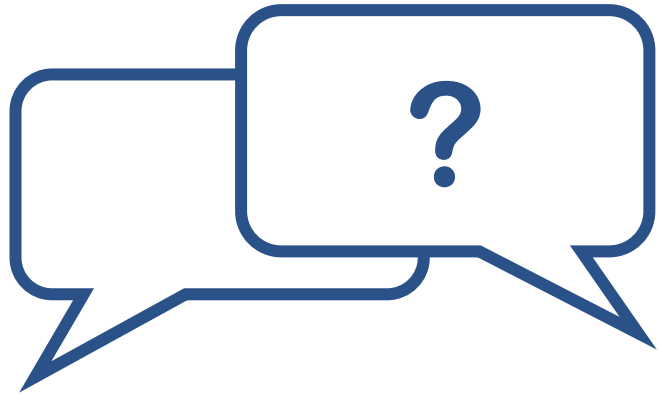
Tendances dans le bulletin quotidien

Selon The Drum, pendant la pandémie de la COVID-19, les attentes accrues des clients et une bonne expérience client (EC) ne suffisaient plus. De nombreuses organisations ont précipité des projets de transformation numérique au cours de la dernière année pour mieux répondre aux besoins des consommateurs qui évoluent rapidement. Cependant, nous nous retrouvons aujourd'hui dans une situation très différente de celle de mars 2020. L'EC doit être plus fluide et personnalisée. Le moment est venu pour les organisations de penser aux outils numériques disponibles non seulement pour maintenir l'efficacité opérationnelle, mais aussi pour amener l'EC vers de nouveaux sommets.

Selon GovTech, les outils de collaboration « se sont avérés des points de réussite cruciaux » qui ont permis aux gouvernements des États et aux administrations locales de maintenir la continuité des services pendant la pandémie de la COVID-19. Aujourd'hui, plus des deux tiers (67 %) des dirigeants gouvernementaux misent sur la modernisation au cours des deux prochaines années, selon une enquête du Center for Digital Government, il est essentiel de veiller à ce que ces efforts appuient les environnements de travail à distance ou hybrides. Pour ce faire, il faudra cependant penser aux outils de collaboration d'une nouvelle façon. Cet article énumère sept stratégies clés pour tirer parti des outils de collaboration à l'appui du travail hybride.



Une étude portant sur quatre gouvernements – deux États et deux administrations locales – qui illustre l'évolution de la méthode agile, d'une approche de développement de logiciels à une application dans la gestion de projets, l'approvisionnement et les services sociaux. Dans toutes les organisations, trois phases d'adoption agile ont émergé : la petite enfance, l'adolescence et l'âge adulte. Selon le rapport, « Agile est une mentalité de changement organisationnel. Processus d'amélioration continue, les méthodes Agile mêmes peuvent évoluer à mesure qu'elles sont utilisées, mises à l'essai et améliorées. »



Nous aimerions connaître votre avis!

Connaissez-vous quelqu'un qui souhaite consulter le rapport des conseils mixtes à l'intention des cadres? Veuillez partager une copie de ce rapport. Si vous n'êtes pas déjà abonné, vous pouvez maintenant vous abonner pour recevoir le rapport à l'intention des cadres en vous inscrivant. Envoyez vos questions à l'adresse info@iccs-isac.org.

Suivi :