Citizen F1RST

OPTIMISÉ PAR
L'Institut
des services axés
sur
les citoyens

Construire une culture sensibilisée à la cybersécurité dans les organisations du secteur public

- Importance de construire une culture sensibilisée à la cybersécurité dans les organismes du secteur public
- Fondements de la culture de cybersécurité dans le secteur public
- Stratégies de mise en œuvre
- Objectifs mesurables et plans d'action
- Défis, risques, possibilités

RAPPORT MENSUEL DE L'EXÉCUTIF DES CONSEILS CONJOINTS

Élaboré par le comité de recherche

Septembre 2023

Images : iStock

1. Importance de construire une culture sensibilisée à la cybersécurité dans les organismes du secteur public

À l'ère de la transformation du numérique, qui s'appuie de plus en plus sur des plateformes numériques, les organisations du secteur public devraient toujours chercher à renforcer leurs cyberdéfenses. Par conséquent, la protection des renseignements critiques étant primordiale, une culture de la cybersécurité permet à tous les employés de constituer une solide ligne de défense.

La cybersécurité n'est pas une destination, mais un voyage permanent. Les agences gouvernementales doivent continuer à faire évoluer leurs stratégies pour rester à la pointe des nouvelles menaces. Une culture de conscience permet de faire preuve d'agilité et de réactivité pour s'adapter au paysage dynamique de la cybersécurité.

Une compréhension globale de la cybersécurité à tous les niveaux crée une approche unifiée de la gestion des risques. Cette prise de conscience organisationnelle ne concerne pas seulement la technologie, mais englobe les politiques, les procédures et les personnes. Une culture sensibilisée à la cybersécurité réduit la probabilité des cyberattaques réussies.

La collaboration au sein des agences gouvernementales, et entre elles, est essentielle pour une stratégie de cybersécurité efficace. Une culture commune favorise la communication, la coopération et la résolution collective des problèmes. Elle constitue un front uni contre les menaces à multiples facettes que représentent les cybercriminels.

Les citoyens confient leurs renseignements personnels et sensibles aux organismes du secteur public. Les effractions peuvent éroder cette confiance et avoir des répercussions durables sur la perception du public. Cultiver une culture de la cybersécurité permet de préserver l'intégrité des systèmes et de préserver la confiance des citoyens.

Sources : Al Hogail, Areej. "Cultivating and assessing an organizational information security culture; an empirical study." International Journal of Security and Its Applications 9, no. 7 (2015): 163–178; Gcaza, Noluxolo, Rossouw von Solms et Joey Jansen van Vuuren. "An Ontology for a National Cyber-Security Culture Environment". In HAISA, pp. 1–10. 2015.

Pourquoi ce rapport est-il important?

L'adoption d'une culture sensible à la cybersécurité dans les organisations du secteur public est une nécessité stratégique à l'ère du numérique. Les cybermenaces évoluent et les mesures de sécurité traditionnelles ne suffisent pas. Comprendre l'importance d'une culture de la sécurité peut conduire à la mise en œuvre de pratiques robustes harmonisées avec les intérêts nationaux.

La collaboration, la sensibilisation et le partage des responsabilités sont essentiels à la mise en place d'un cadre de cybersécurité solide. Ce rapport met en lumière les mécanismes qui favorisent cet environnement. Les renseignements fournis visent à aider les décideurs politiques à élaborer des lois, des règlements et des mesures incitatives qui soutiennent une approche globale de la cybersécurité.

Une approche cohérente de la cybersécurité à l'échelle du gouvernement fait partie intégrante de la protection des intérêts nationaux. Le présent rapport contribue à cet objectif en mettant en évidence les éléments essentiels d'une culture sensibilisée à la cybersécurité. Il sert de feuille de route aux organisations du secteur public pour harmoniser leurs pratiques en matière de cybersécurité avec les objectifs gouvernementaux plus larges.

Quels sont les éléments couverts par ce rapport?

Ce rapport comprend les éléments suivants :

- Importance de construire une culture sensibilisée à la cybersécurité dans les organismes du secteur public
- Fondements de la culture de cybersécurité dans le secteur public
- Stratégies de mise en œuvre
- Objectifs mesurables et plans d'action
- Défis, risques, possibilités

2. Fondements de la culture de cybersécurité dans le secteur public

L'instauration d'une culture de la cybersécurité au sein des organisations gouvernementales est un effort multidimensionnel qui transcende la technologie. Examinons les principaux piliers fondamentaux qui contribuent à façonner une telle culture.

Responsabilité partagée entre les ministères : La cybersécurité n'est pas confinée au département des technologies de l'information; il s'agit plutôt d'un effort collaboratif. Chaque ministère et agence doit être au fait de son rôle dans la protection de ses actifs numériques et de ses données publiques.

Éducation et formation holistiques : La formation et les initiatives éducatives continues sont essentielles pour garantir que le personnel à tous les niveaux possède les compétences nécessaires pour cerner et atténuer les menaces en matière de cybersécurité. Le programme doit être adaptable et répondre aux différents rôles au sein de l'organisation.

Engagement en matière de leadership : La pierre angulaire d'une culture de la cybersécurité est l'engagement sans équivoque de la part des dirigeants. Leur participation active aux initiatives en matière de cybersécurité permet non seulement de donner le ton à l'organisation, mais aussi d'assurer l'affectation des ressources et l'application des politiques.

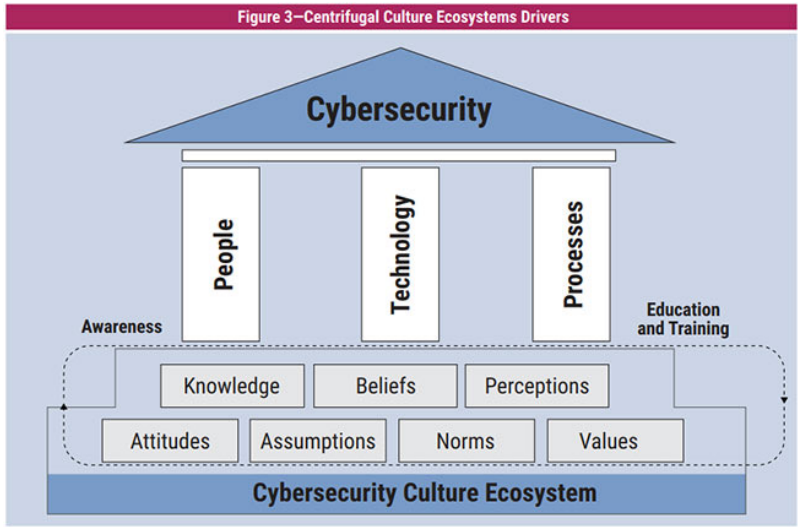
Des politiques robustes et des procédures opérationnelles normalisées (PON) : Des politiques clairement articulées et largement diffusées fournissent un cadre structurel pour des comportements favorisant la cybersécurité. Ils doivent être accessibles, faciles à comprendre et régulièrement mis à jour pour s'adapter à l'évolution du paysage des menaces.

Solutions technologiques centrées sur la personne : Si la technologie est un outil indispensable, son efficacité est maximale lorsqu'elle est adaptée aux éléments humains de l'organisation. L'objectif est d'intégrer des solutions technologiques intuitives, conviviales et adaptées aux activités quotidiennes.

Responsabilité et transparence : Il est essentiel de gagner et de conserver la confiance du public. Cet objectif peut être atteint grâce à des pratiques transparentes et en tenant tous les membres responsables de leurs actions en matière de cybersécurité.

Coopération interinstitutions : La collaboration entre différents organismes gouvernementaux amplifie l'efficacité des mesures de cybersécurité. Une stratégie unifiée, fondée sur des ressources et des renseignements communs, renforce la capacité collective du gouvernement à contrecarrer les cyberattaques.

Examinez le cadre de l'écosystème de la culture de cybersécurité proposé par l'association Information Systems Audit and Control Association (ISACA) ci-dessous.



Sources : Möller, Dietmar PF. Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Vol. 103. Springer Nature, 2023.; ISCACA: Implementing a Cybersecurity Culture (2019); Uchendu, Betsy, Jason RC Nurse, Maria Bada, and Steven Furnell. "Developing a cyber security culture: Current practices and future needs." Computers & Security 109 (2021): 102387.

3. Stratégies de mise en œuvre d'une culture sensibilisée à la cybersécurité

La mise en place d'une culture de la cybersécurité dans les organismes du secteur public nécessite une approche structurée et stratégique. L'exploitation des meilleures pratiques, l'adaptation de la formation et la mise en place d'une collaboration intersectorielle sont des éléments fondamentaux de cette transformation.

Sensibilisation et éducation

— La sensibilisation à la cybersécurité doit commencer au sommet de la hiérarchie. La direction doit être bien informée et s'engager à défendre la cause, à l'harmoniser avec les objectifs de l'organisation et à fournir les ressources nécessaires à une formation et à un enseignement efficaces.

— Il est essentiel d'adapter la formation à la cybersécurité aux différents rôles au sein de l'organisation. Du personnel de première ligne aux professionnels de l'informatique, chacun doit comprendre ses responsabilités spécifiques et les implications de leurs actions sur la cybersécurité globale.

Technologie et infrastructure

Il est primordial de mettre en œuvre des solutions technologiques conformes aux objectifs de cybersécurité de l'organisation. Il ne s'agit pas seulement de déployer des outils de pointe, mais aussi de veiller à ce qu'ils soient configurés correctement, entretenus régulièrement et intégrés de manière transparente dans l'infrastructure existante.

— La cybersécurité ne consiste pas seulement à se défendre contre les menaces extérieures. Les contrôles internes et les systèmes de surveillance sont tout aussi essentiels. La mise en œuvre de procédures d'authentification solides, des vérifications de sécurité régulières et de plans de réponse aux incidents contribue au maintien d'un environnement sécurisé.

Politique et gouvernance

— Des politiques et des procédures claires et applicables constituent le pilier d'une culture de la cybersécurité. Ces politiques doivent être régulièrement mises à jour pour tenir compte de l'évolution des menaces et des exigences réglementaires et doivent être communiquées efficacement à l'ensemble du personnel.

— Les structures de gouvernance qui facilitent la collaboration interministérielle et garantissent la responsabilité à tous les niveaux sont essentielles. Un organe de gouvernance dédié à la cybersécurité peut superviser la mise en œuvre, le suivi et l'amélioration continue des pratiques de cybersécurité dans l'ensemble de l'organisation.

Collaboration et partage d'informations

— Les plateformes de collaboration qui permettent aux organisations du secteur public d'échanger des renseignements sur les menaces, des bonnes pratiques et des ressources renforcent la défense collective contre les cyberadversaires.

— La confiance est essentielle pour une collaboration efficace. L'élaboration d'accords formels, la garantie de la confidentialité et la création de canaux de communication sécurisés encouragent les organisations à effectuer un échange sécurisé de renseignements sans craindre de compromettre des données sensibles.

Sources : Georgiadou, Anna, Spiros Mouzakitis, and Dimitris Askounis. "Detecting insider threat via a cyber-security culture framework." Journal of Computer Information Systems 62, no. 4 (2022): 706–716.

4. Objectifs mesurables et plans d'action

Des objectifs mesurables et des plans d'action constituent le plan directeur de la mise en œuvre d'une culture de la cybersécurité. La définition d'objectifs clairs et d'étapes réalisables, soutenue par un suivi et un examen régulier, garantit que la stratégie est effectivement mise en pratique.

Définir des objectifs clairs, spécifiques et mesurables en matière de cybersécurité harmonisés avec les objectifs de l'organisation. Ces objectifs doivent être à la fois à court et à long terme. Ils doivent être communiqués à l'ensemble de l'organisation et être liés à des mesures de rendement individuel. Des évaluations régulières permettent de suivre les progrès réalisés et de procéder aux ajustements nécessaires.

Créer des plans d'action qui décrivent les étapes à suivre pour atteindre chaque objectif. Ces plans doivent inclure des échéances, des parties responsables et les ressources nécessaires. Les plans d'action favorisent la responsabilisation et permettent à chacun de connaître son rôle dans la réalisation des objectifs de cybersécurité. La planification collaborative, impliquant différents ministères, améliore l'exhaustivité et l'efficacité de ces plans.

Mettre en œuvre des mécanismes de suivi afin d'évaluer régulièrement l'état d'avancement des plans d'action. Un suivi régulier permet de savoir ce qui fonctionne et ce qui doit être amélioré. Il permet d'intervenir en temps utile et de veiller à ce que les plans restent harmonisés avec l'évolution du paysage de la cybersécurité. Les boucles de rétroaction impliquant toutes les parties prenantes enrichissent le processus de suivi et favorisent l'amélioration continue.

Favoriser une culture de l'amélioration et de l'apprentissage continus. La cybersécurité est un domaine dynamique, et une approche statique peut rapidement devenir obsolète. Encourager une culture qui accepte le changement, qui tire les leçons des succès et des échecs et qui cherche constamment à s'améliorer, permet à l'organisation de rester agile et réactive face aux menaces émergentes.

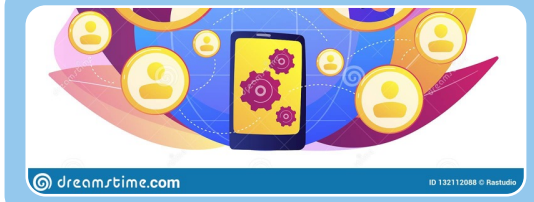
La collaboration entre les différentes entités gouvernementales est essentielle pour parvenir à une approche unifiée de la cybersécurité. Des objectifs communs et des plans d'action coordonnés permettent une approche synergique de la cybersécurité. Des réunions interagences régulières, des mécanismes de communication harmonisés et des projets de collaboration renforcent la capacité collective à répondre aux cybermenaces. Cette collaboration s'étend au-delà du gouvernement, impliquant le secteur privé et les partenaires internationaux, le cas échéant.

Encourager l'innovation et la recherche au sein du secteur public afin de se tenir au courant des dernières tendances et solutions en matière de cybersécurité. L'investissement dans la recherche et le développement permet au secteur public de garder une longueur d'avance en matière de cybersécurité. Tisser de partenariats avec le monde universitaire, le secteur privé et d'autres institutions de recherche favorise l'innovation. La mise à jour régulière des stratégies sur la base des résultats de la recherche garantit que le secteur public reste un acteur actif dans l'élaboration de l'avenir de la cybersécurité.

Sources : Trim, P. and Upton, D., 2016. Cyber security culture: Counteracting cyber threats through organizational learning and training. Routledge; Gcaza, Noluxolo, Rossouw von Solms, and Joey Jansen van Vuuren. "An Ontology for a National Cyber-Security Culture Environment". In HAISA, pp. 1–10. 2015; Ghernaouti, Solange, and Bastien Wanner. "Research and education as key success factors for developing a cybersecurity culture." Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden (2018): 539–552.

5. Défis, risques et possibilités

Cerner et relever les différents défis liés à la mise en place d'une culture sensibilisée à la cybersécurité. Ces défis peuvent inclure la résistance au changement, des ressources limitées et la complexité de l'intégration des différents éléments de cybersécurité. Un dialogue ouvert, des ressources dédiées et un engagement fort de la part des dirigeants peuvent atténuer ces difficultés et faciliter une transition en douceur.



Repérer et atténuer les risques liés à la transformation de la cybersécurité. Les risques peuvent inclure des lacunes potentielles en matière de sécurité pendant la transition, des conflits potentiels avec les réglementations existantes et des conséquences imprévues sur d'autres fonctions de l'organisation. Un cadre solide de gestion des risques comprenant des évaluations régulières des risques, des stratégies d'atténuation et des mécanismes de suivi permet de gérer ces risques de manière efficace.

Saisir les possibilités qu'une culture de la cybersécurité apporte aux organisations du secteur public. Ces possibilités peuvent inclure une meilleure collaboration, une confiance accrue du public et une meilleure résistance aux cybermenaces. Pour tirer parti de ces possibilités, il faut adopter une approche proactive, s'améliorer en permanence et s'harmoniser avec des stratégies gouvernementales plus larges.

Reconnaître le rôle des parties prenantes externes dans l'élaboration du paysage de la cybersécurité. Les partenariats avec le secteur privé, les organismes internationaux et d'autres entités gouvernementales offrent des possibilités d'apprentissage mutualisé et de collaboration. Ces relations doivent être entretenues et gérées efficacement afin d'exploiter les forces et les perspectives uniques de chaque partie.

Cultiver un état d'esprit qui considère la cybersécurité comme un catalyseur plutôt que comme un obstacle. Faire passer la perception de la cybersécurité d'un obstacle à un outil permettant d'atteindre les objectifs de l'organisation favorise l'acceptation et l'intégration dans les opérations quotidiennes. Ce changement d'état d'esprit encourage l'innovation, améliore la collaboration et crée une organisation plus résiliente et plus souple.

Sources : Corradini, Isabella. Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology. Vol. 284. Springer Nature, 2020.

Pour de plus amples renseignements

- Nagyfejeo, Eva, and Basie Von Solms. “Why do national cybersecurity awareness programmes often fail.” International Journal of Information Security and Cybercrime 9, no. 2 (2020): 18–27.
- Christine, Debora, and Mamello Thinyane. “Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies.” (2020).
- Teoh, Chooi Shi, and Ahmad Kamil Mahmood. “Cybersecurity workforce development for digital economy.” The Educational Review, USA 2, no. 1 (2018): 136–146.
- Nurse, Jason. “A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK.” (2017).
- Murray, Peter J., and Roger J. Ward. “Promoting enterprise risk management (ERM) and governance, risk and compliance (GRC) for managing cybersecurity risks.” (2018).
- Saputra, Pradipta Nindyan, Arfin Sudirman, Obsatar Sinaga, Wahyu Wardhana, and Nurul Hayana. “Addressing Indonesia’s Cyber Security through Public-Private Partnership (PPP).” Central European Journal of International & Security Studies 13, no. 4 (2019).

Autres articles marquants :

- Hoggard, Amy. “Comparing Canadian and American cybersecurity awareness levels: Educational strategies to increase public awareness.” PhD diss., Utica College, 2014.
- Mishra, Alok, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, and Asif Qumer Gill. “Attributes impacting cybersecurity policy development: An evidence from seven nations.” Computers & Security 120 (2022): 102820.

Référentiel de recherche

Accédez au référentiel de recherche de l’Institut des services axés sur les citoyens.

Entrées récentes dans le référentiel de recherche :

Définir les biais dans l’Intelligence artificielle (IA) et la prestation de services publics

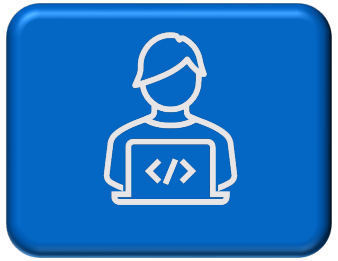
Ce rapport comprend les éléments suivants :

- Importance de la définition des biais dans l’IA et la prestation de services publics
- Repérer les types et les sources de biais dans l’IA
- L’intersection du biais et de l’éthique dans l’IA au sein du gouvernement
- Stratégies et mesures pour atténuer les préjugés

Tendances dans le bulletin d'information quotidien

Service Canada travaille avec diligence pour offrir des services de haute qualité, simples, faciles d'accès et sécurisés aux Canadiens, quel que soit leur lieu de résidence. Au fur et à mesure que la technologie progresse et que les attentes des clients en matière de prestation de services évoluent, le gouvernement du Canada prend des mesures pour moderniser davantage ses méthodes de prestation et les services disponibles.

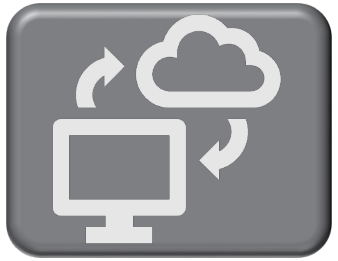
Dans le cadre de ces efforts de modernisation, Service Canada a amélioré le service en ligne « Mon dossier Service Canada (MSCA) » afin de permettre à toute personne possédant un compte de trouver son numéro d'assurance sociale (NAS) en ligne et en toute sécurité.



Terry Beech, le tout premier ministre fédéral des services aux citoyens, a récemment déclaré à CBC News que l'une des priorités de sa nouvelle fonction sera de rendre les services du gouvernement fédéral « numérique d'abord » et « numérique dès leur conception »

Il a également fait part de sa volonté d'utiliser les nouvelles technologies telles que l'IA pour améliorer la manière dont le gouvernement fournit des services aux Canadiens.

« Je suis sûr que certaines personnes s'inquiéteront lorsque nous parlerons de numérique d'abord », a constaté M. Beech. « Numérique d'abord ne signifie pas que nous n'aurons pas d'options en personne ou par téléphone



Le Canada est devenu le premier pays au monde à approuver l'exploitation commerciale d'un opérateur CFA.

Cela signifie que le Canada sera le premier pays à disposer de services Wi-Fi à 6 GHz de puissance standard commercialement opérationnels d'ici quelques mois.

Cette désignation a été annoncée par l'Innovation, Science et Développement économique Canada (ISDE), un service du gouvernement canadien, qui a désigné Qualcomm comme le premier « administrateurs de coordonnateurs de fréquences automatisés » (ACFA) du pays. Il s'agit également d'une première collaboration du genre pour Qualcomm et pour l'industrie du Wi-Fi.

Nous serions ravis de savoir ce que vous en pensez!

Connaissez-vous quelqu'un qui pourrait être intéressé par le rapport à l'intention des cadres du Conseil conjoint? Veuillez leur envoyer une copie de ce rapport. Si vous n'êtes pas encore abonné, vous pouvez désormais vous inscrire pour recevoir le rapport à l'intention des cadres. Faites parvenir vos questions à info@iccs-isac.org.

Suivez-nous :