digital NEW BRUNSWICK

# Assurer notre avenir numérique en toute sécurité

**Finances et Conseil du Trésor**
**Bureau du chef de l'information**



New Nouveau Brunswick

**Stratégie de cybersécurité**

# Table des matières

# Aider à bâtir un Nouveau-Brunswick numérique

**La cybersécurité est un élément clé dans la création d'un Nouveau-Brunswick numérique. La présente stratégie de cybersécurité établit un cadre visant à assurer la sécurité et la pérennité de l'information et des systèmes servant à tous les Néo-Brunswickois, que ce soit au travail, à la maison ou dans les loisirs.**

**Notre approche se résume au principe suivant : en savoir assez pour bien protéger. Ainsi, afin d'atteindre nos objectifs, nous devons bien connaître nos activités et exercer une « juste protection », parfaitement adaptée, sans être exagérée.**

## Où en est la cybersécurité aujourd'hui?

Le terme cybersécurité englobe les « mesures prises pour prévenir l'accès non autorisé ou l'atteinte aux données ». La technologie est en constante évolution et influence nos modes de vie : les téléphones intelligents et technologies médicales salvatrices, notamment, nous sont aujourd'hui indispensables. Les malfaiteurs profitent toutefois aussi de la technologie, par exemple pour s'emparer de numéros de cartes de crédit ou prendre des données en otage. Grâce aux nouvelles technologies, comme l'intelligence artificielle, les pirates lancent des attaques plus poussées et difficiles à contrer.

## Notre cyberavenir – fondé sur la confiance, l'agilité et les solutions

Nous devons miser sur une cybersécurité forte pour instaurer la confiance dans une société numérique. Les mécanismes de cybersécurité doivent être simples et intégrés à tous les services du GNB. Nous serons agiles. Nous parerons rapidement les cyberattaques et nous serons très réactifs à l'évolution des besoins des citoyens. Par-dessus tout, notre approche aidera les citoyens à accéder aux

## Nos objectifs pour un Nouveau-Brunswick cybersécuritaire

1. **Protéger l'information et les systèmes du Nouveau-Brunswick**
   - Une information confidentielle, fiable et accessible aux citoyens, au besoin
   - Des mécanismes de cybersécurité efficaces et cohérents dans l'ensemble du gouvernement
2. **Adopter une approche équilibrée risques-avantages**
   - Une culture de la cybersécurité à l'échelle de la province
   - Des décisions en matière de cybersécurité fondées sur une information fiable
3. **Protéger mieux, plus intelligemment et plus rapidement**
   - Des solutions de cybersécurité de plus en plus automatisées et intégrées
   - Un GNB qui s'adapte rapidement à l'évolution des menaces et des besoins
4. **Instaurer la cyberconfiance**
   - Des citoyens convaincus de recevoir des services numériques en toute sécurité de la part du GNB
5. **Former, préserver, fidéliser**
   - Des employés tous formés sur les pratiques de cybersécurité
   - Des employés possédant les compétences nécessaires pour assurer la sécurité de l'information gouvernementale

services en toute sécurité, de manière simple et conviviale.

- Un GNB offrant un milieu de travail séduisant pour les professionnels qualifiés de la cybersécurité

# Où s'en va le Nouveau-Brunswick?

**Nous sommes à l'ère du numérique. Nos façons de communiquer, d'aller chercher de l'information et de faire des affaires sont révolutionnées à jamais. Pour faire nos achats, réserver des voyages, effectuer des opérations bancaires ou payer des factures, nous nous attendons désormais à un accès instantané. Nous voulons une information en temps quasi réel et facile à consulter. Le numérique joue déjà un rôle prépondérant dans nos vies et l'économie du Nouveau-Brunswick, rôle appelé à grandir. Voilà une occasion à saisir!**

L'accès des Néo-Brunswickois à leurs renseignements personnels en ligne doit être sûr et sécurisé. Il est essentiel que l'information gouvernementale et les renseignements personnels des citoyens soient protégés pour prévenir les accès non autorisés. L'exactitude et la disponibilité en temps opportun de ces données sont tout aussi cruciales.

La cybersécurité est l'un des sept grands volets de la stratégie numérique du GNB. Elle aide la société

À l'ère du numérique, les Néo-Brunswickois souhaitent par exemple utiliser leur téléphone intelligent pour renouveler leur permis de conduire ou consulter leurs résultats d'examens médicaux. Ils veulent le faire à tout moment, de partout et depuis n'importe quel appareil. Dans cet esprit, nous modernisons la façon de fournir les services à la population par la mise en œuvre d'une stratégie intitulée « Nouveau-Brunswick numérique ».

## Quel est le bien-fondé d'une stratégie de cybersécurité?

Internet et les médias sociaux offrent d'excellents outils aux cybercriminels. Que ce soit par le vol de numéros de carte de crédit ou des virus informatiques, leurs moyens de frapper sont nombreux. Les pirates informatiques ont accès aux dernières technologies, et leurs méthodes évoluent constamment.

Des incidents de cybersécurité – tentatives réussies d'accès illicite à un ordinateur ou à des systèmes informatiques – se produisent tous les jours (voir la figure 1) au sein de gouvernements et d'entreprises. Or, mal préparés, nous pourrions mettre du temps à découvrir les actes de piratage dont nous serions victimes.

Le message est clair. Les cybercriminels s'adaptent constamment aux nouvelles technologies. Les gouvernements et les entreprises doivent être tout aussi rusés pour contrer cette menace et protéger leur information.

néo-brunswickoise à adopter le numérique de manière sûre et sécurisée.

## Quelle est notre vision de la cybersécurité?

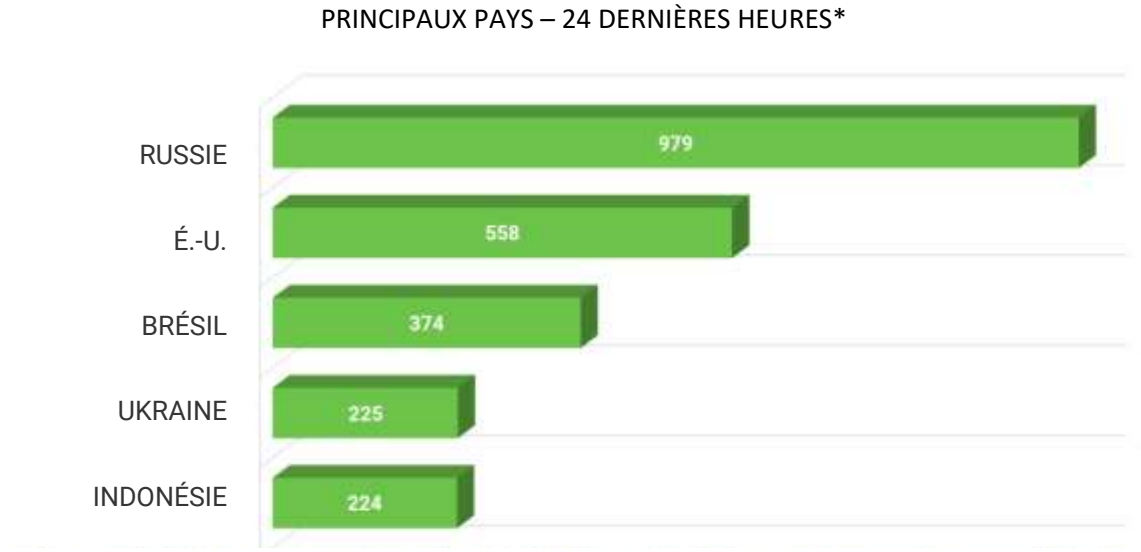
**La stratégie de cybersécurité appuiera le Nouveau-Brunswick numérique. Notre vision : mettre en place un environnement sûr et fiable pour l'essor du Nouveau-Brunswick numérique.**

La stratégie Nouveau-Brunswick numérique repose sur cinq principes, appliqués intégralement dans le cadre de la cyberstratégie :

- Nous plaçons les citoyens et les entreprises au cœur de nos activités.
- Nous utilisons des renseignements exacts et fiables pour prendre des décisions fondées sur des données probantes.
- Nous nous adaptons rapidement au changement et nous nous améliorons de façon itérative.
- Nous travaillons dans le cadre de partenariats de confiance.
- Nous adoptons une vision globale.

En bref, le Nouveau-Brunswick misera sur une cybersécurité fiable, agile et axée sur les solutions.

## Figure 1 – Cyberattaques en temps réel – GNB (23 janvier 2019, à 8 h 30 [HA])




**Pays sources (et non désignés comme commanditaires) des cyberattaques.

## Confiance

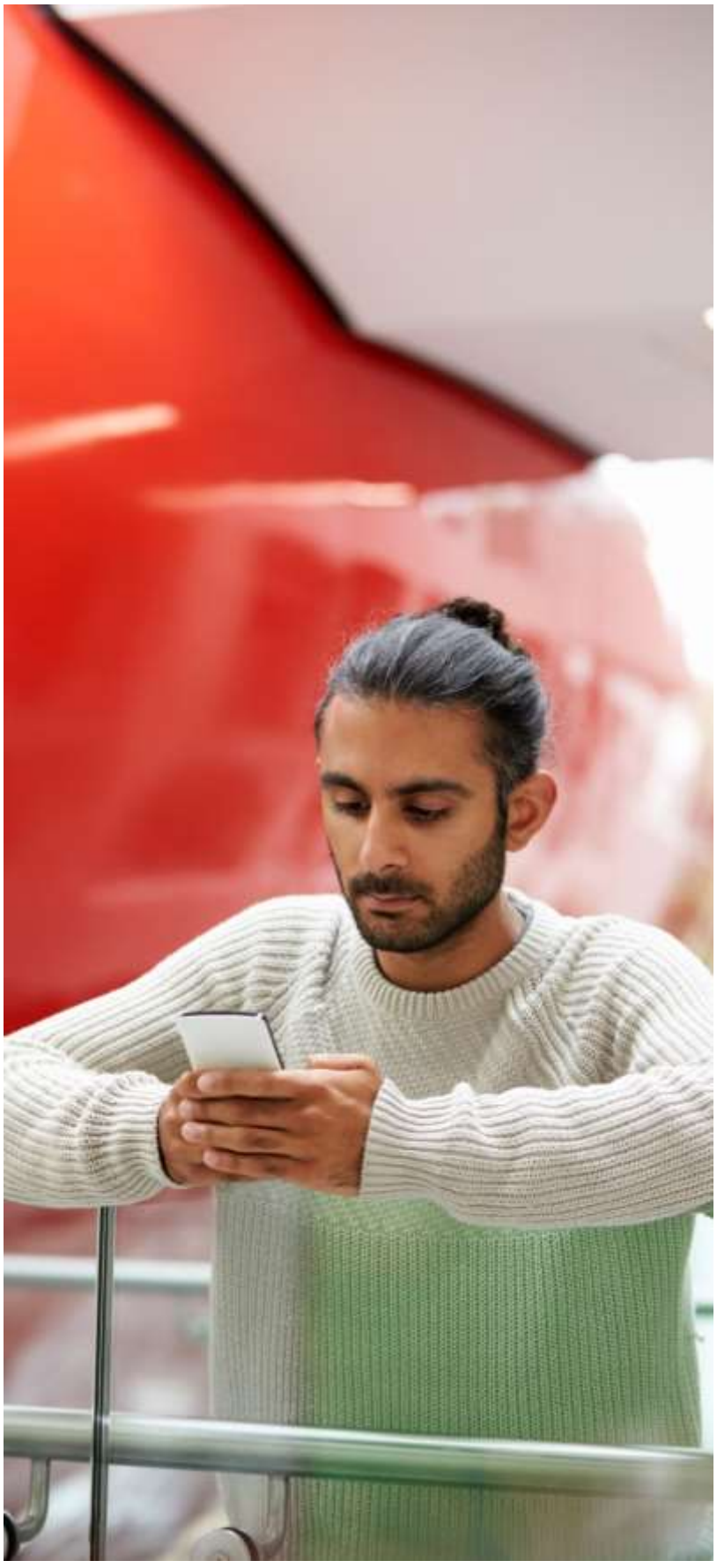
La stratégie vise à offrir une cybersécurité qui aide les citoyens et les entreprises à prospérer dans un monde numérique. Cela requiert de la confiance. Cette confiance part d'un **leadership et d'une direction forts**. Ainsi, les gestionnaires doivent prôner la collaboration et la communication entre tous les ministères, à tous les niveaux. Une approche cohérente de la cybersécurité dans l'ensemble du gouvernement demandera par ailleurs un solide travail d'équipe. Voilà comment nous instaurerons la confiance avec toutes les parties prenantes.

## Agilité

La technologie évolue rapidement et les cybercriminels suivent le rythme. Nous allons relever les défis de la cybersécurité rapidement et de manière itérative, en nous améliorant au fil du temps. Nous devons viser l'adoption de solutions intelligentes recourant aux nouvelles technologies, comme l'intelligence artificielle, pour automatiser notre protection contre les cyberattaques. Notre réponse doit être rapide et efficace, dans un contexte de perpétuelle évolution de la menace informatique et des lois sur la protection de la vie privée.

## Solutions

Dans le développement de solutions de cybersécurité, nous prendrons en compte les besoins des gens et non seulement les préoccupations technologiques. Nous devons trouver le juste équilibre et prévenir le risque émergent par des solutions qui répondent aux besoins des citoyens et des entreprises.



# Comment est née la stratégie de cybersécurité?

Elle a avant tout été pensée pour notre clientèle, dans le cadre d'ateliers et de rencontres tenus sur plusieurs mois. Voilà qui nous a permis de comprendre notre situation actuelle et souhaitée en matière de cybersécurité, et aussi de nous fixer des objectifs réalistes.

# Qui sont les acteurs clés?

Tout le monde a un rôle à jouer dans la cybersécurité. En contribuant tous, nous réduisons collectivement les risques et augmentons les avantages.

## Gouvernement du Nouveau-Brunswick (GNB)

Le gouvernement du Nouveau-Brunswick est responsable de la protection des données des Néo-Brunswickois dont il a la charge. Certains ministères et organismes du GNB ont des responsabilités plus précises.

## Finances et Conseil du Trésor (FCT)

Le ministère des Finances et du Conseil du Trésor est chargé de fournir des services liés aux stratégies, aux politiques, à la surveillance et aux rapports à tous les autres ministères et organismes du GNB.

## Service Nouveau-Brunswick

Service Nouveau-Brunswick fournit un soutien opérationnel pour la protection des biens du GNB en appliquant la stratégie, les politiques et les orientations du ministère des Finances et du Conseil du Trésor.

## Ministère la Sécurité publique (MSP)

Le ministère de la Sécurité publique voit à la sécurité nationale et générale de la population, à la gestion des urgences, à l'application de la loi et à la sécurité des infrastructures essentielles.

## Ministère des Transports et de l'Infrastructure (MTI)

Le ministère des Transports et de l'Infrastructure est responsable de la sécurité des édifices gouvernementaux.

## CyberNB

CyberNB (une initiative d'Opportunités NB) aide à renforcer les capacités du Nouveau-Brunswick en matière de cybersécurité par l'innovation collaborative entre le gouvernement, le secteur privé, le milieu universitaire et d'autres secteurs.

## Ministère de l'Éducation postsecondaire, de la Formation et du Travail (EPFT) et ministère de l'Éducation et du Développement de la petite enfance (EDPE)

EPFT et EDPE forment les Néo-Brunswickois en ce qui a trait à la cybersécurité et à la culture numérique.

## Employés du GNB

Les employés du GNB sont tenus de se conformer aux politiques et normes de cybersécurité, qui les aideront à rester en sécurité et à fournir des services sécurisés aux citoyens.

## Communauté des affaires

Il incombe aux entreprises de protéger leurs appareils et leur information, ainsi que d'assurer le soutien des infrastructures essentielles, comme celles vouées aux télécommunications, à l'énergie, aux transports, à l'eau et à l'alimentation.

## Citoyens

Nous sommes tous responsables de notre protection en ligne, à la maison comme au travail. Nous devons tenir nos appareils à jour et ne communiquer notre information personnelle qu'à des personnes de confiance.

# Quel est l’impact pour les Néo-Brunswickois?

**La stratégie numérique du GNB s’adresse à tous les Néo-Brunswickois.** Qu’ils soient en ligne ou non, les citoyens constateront des améliorations à leur vie quotidienne.

Nos mesures de cybersécurité empêcheront la consultation et la modification de leur information sans leur consentement, mais leur permettront aussi d’accéder à leurs données quand ils en ont besoin.

# Quels sont nos objectifs?

**Voici les objectifs stratégiques et les résultats attendus de la stratégie de cybersécurité.**

## 1. Protéger l'information et les systèmes du Nouveau-Brunswick

**Résultats et indicateurs de rendement clés (IRC)**

- Des mécanismes de cybersécurité efficaces et cohérents dans l'ensemble du gouvernement.
  IRC – % des contrôles annuels effectués dans les délais

- Les politiques favorisent l'imputabilité et la transparence des mesures de cybersécurité.
  IRC – % des examens annuels des politiques/directives réalisés dans les délais

- Un programme de cybersécurité rigoureux fournit des orientations à l'ensemble du GNB.
  IRC – % des évaluations de cybersécurité prévues effectuées dans les délais

**Actions**

- Procéder à des évaluations du niveau de maturité et de vulnérabilité afin d'améliorer continuellement le programme de cybersécurité du GNB.
- Diffuser des stratégies visant l'Internet des objets (IdO), les technologies mobiles, l'infonuagique et les technologies émergentes.
- Adopter des outils de cybersécurité normalisés dans l'ensemble du GNB.
- Élaborer un tableau de bord équilibré de la cybersécurité.
- Mettre sur pied un modèle et une politique de cybersécurité similaires à ceux de la santé et de la sécurité.

## 2. Adopter une approche équilibrée risques-avantages

**Résultats et indicateurs de rendement clés (IRC)**

- Le risque en matière de cybersécurité est inclus au processus décisionnel.
  IRC – % des examens annuels du risque réalisés dans les délais

- Les gestionnaires sont formés quant à la gestion du cyberrisque.
  IRC – % de gestionnaires formés sur la gestion du cyberrisque

- Les cadres supérieurs sont informés sur le cyberrisque grâce à des rapports produits en temps utile.
  IRC – % des rapports de cybersécurité présentés dans les délais

**Actions**

- Établir un registre des cyberrisques.
- Cibler de bonnes pratiques de gestion du risque.
- Mener une évaluation gouvernementale du risque visant les appareils intelligents du GNB (IdO).
- Effectuer une évaluation gouvernementale du risque en matière de technologies mobiles.

## 3. Protéger mieux, plus intelligemment et plus rapidement

**Résultats et indicateurs de rendement clés (IRC)**

- Les solutions de cybersécurité sont intégrées et s'appliquent à tous les incidents en matière de cybersécurité au gouvernement.
  IRC – % des incidents entièrement traités par le Centre des opérations de sécurité

- Les cyberattaques sont détectées immédiatement et la réponse est de plus en plus automatisée.

IRC – % des incidents de cybersécurité résolus dans les délais

- Le GNB dispose d'un plan de reprise après sinistre continuellement mis à jour.
  IRC – % des plans de reprise après sinistre prévus examinés dans les délais

**Actions**

- Actualiser en permanence la stratégie et la feuille de route du Centre des opérations de sécurité du GNB.
- Élargir le champ d'action du Centre des opérations de sécurité aux quatre parties du gouvernement, et fournir des renseignements utilisables sur les menaces.
- Actualiser en permanence la stratégie et la feuille de route du GNB pour la reprise après sinistre.
- Améliorer le processus gouvernemental de gestion des incidents de cybersécurité.
- Élaborer une stratégie de gestion des cybercrises pour faire face aux nouvelles cyberattaques.

## 4. Instaurer la cyberconfiance

**Résultats et indicateurs de rendement clés (IRC)**

- Le GNB collabore avec les entreprises et les universités par l'intermédiaire de CyberNB et d'autres entités.
  IRC – Nombre de partenariats fructueux avec des établissements universitaires et des entreprises

- Le GNB collabore de manière transparente avec d'autres administrations du Canada et d'ailleurs.
  IRC – Des partenariats interprovinciaux/fédéraux fructueux

**Actions**

- Renforcer nos liens avec différentes parties prenantes pour améliorer nos capacités en cybersécurité et mieux protéger notre réseau.
- Collaborer avec le Canadian Institute of Cyber Security et le Centre canadien pour la cybersécurité.
- Explorer les possibilités avec CyberNB en matière de formation, de partage d'information et d'établissement de meilleures pratiques.

## 5. Former, préserver, fidéliser

**Résultats et indicateurs de rendement clés (IRC)**

- Tous les employés reçoivent une formation régulière sur les bonnes pratiques de cybersécurité.
  IRC – % des employés du GNB formés en matière de cybersécurité

- Les talents en matière de cybersécurité font partie d'un plan stratégique de gestion des talents.
  IRC – % des démarches de planification de carrière des employés en cybersécurité réalisés dans les délais

**Actions**

- Mettre en place un réseau d'excellence pour les professionnels de la cybersécurité du GNB.
- Élaborer et mettre en œuvre un programme de formation en cybersécurité pour l'ensemble du GNB.
- Offrir une formation en cybersécurité fondée sur le rendement.

# Quels sont les défis et les possibilités?

**De nombreux défis se posent à nous, alors que nous cherchons à instaurer la confiance et à protéger les données des citoyens. Chacun de ces défis représente aussi une occasion de mieux servir les citoyens.**

## Défi : méconnaissance de la cybersécurité

Le succès d'un programme de cybersécurité repose sur la communication de pratiques efficaces dans toute l'organisation.

**Possibilité : La mise en œuvre de la stratégie de cybersécurité comprendra la sensibilisation et l'éducation, les paramètres de mesure et les responsabilités appropriées.**

## Défi : financement

Un investissement adéquat est nécessaire pour atteindre les objectifs de la stratégie de cybersécurité.

**Possibilité : La stratégie de cybersécurité cible les aspects clés nécessitant des investissements pour offrir un bon niveau de protection au GNB.**

## Défi : manque de préparation de l'organisation

La GNB doit attirer et conserver les meilleurs éléments pour atteindre ses objectifs opérationnels. Nous utiliserons la technologie pour combler les lacunes en matière de dotation en personnel et de compétences dans le domaine de la cybersécurité. Le GNB devra aussi miser sur des éléments fondamentaux comme l'infrastructure et les mécanismes d'intégration, pour mettre en œuvre sa stratégie de cybersécurité.

**Possibilité : Une approche novatrice de recrutement et de formation permettra de promouvoir la cybersécurité et de bien préparer l'organisation.**

## Défi : tendances mondiales/technologies perturbatrices en cybersécurité

Le GNB doit suivre l'évolution des tendances et des technologies mondiales.

**Possibilité : La stratégie de cybersécurité permettra de prendre des décisions plus rapides et éclairées concernant les nouvelles technologies.**

## Défi : durabilité

Les gouvernements et l'environnement de sécurité sont en constante évolution. Nous devons nous adapter continuellement pour maintenir notre vision.

**Possibilité : La stratégie de cybersécurité sera réexaminée régulièrement en fonction de l'évolution des besoins du gouvernement. Nous veillerons à ce que les procédures soient bien documentées et que les rôles et responsabilités des employés soient clairement définis.**

# Comment gérerons-nous le cyberrisque?

Comme tout gouvernement, le GNB gère les risques dans les domaines de la santé et de la sécurité, des finances, des ressources humaines, de l'environnement, etc. Nous aiderons les responsables de secteurs du GNB à cibler et à gérer leur propre cyberrisque.

**Notre travail en ce sens :**

- **Voir à l'orientation et au contrôle au sein du GNB pour protéger l'information et s'assurer que les employés travaillent en ligne en toute sécurité**
- **Surveiller les tendances en matière de sécurité**
- **Rendre compte des risques aux parties prenantes responsables**
- **Affiner la cyberstratégie et les politiques à venir selon nos apprentissages**
- **Rendre la stratégie compréhensible aux décideurs**

# Comment savoir si nous sommes sur la bonne voie?

Nous avons une emprise sur des objectifs réalistes et mesurables, qui sont au cœur de notre cyberstratégie. Notre approche suppose des objectifs accessibles à tous, ainsi que des mesures simples illustrant nos progrès.

# Conclusion

La stratégie de cybersécurité aidera à créer un Nouveau-Brunswick numérique cybersécurisé.

**Elle décrit la manière dont nous :**

- **instaurerons la confiance auprès de nos utilisateurs et les parties prenantes au GNB et ailleurs;**
- **serons agiles et nous adapterons à l'évolution des besoins gouvernementaux, des technologies et de la menace;**
- **axerons notre travail sur des solutions et contribuerons à faire avancer le gouvernement;**
- **veillerons à ce que les mesures appropriées soient adoptées pour assurer la protection adéquate.**

Cette stratégie permettra au Nouveau-Brunswick de rentabiliser au maximum ses investissements dans la cybersécurité.