



# LES RISQUES DU STATU QUO NUMÉRIQUE

Comment les gouvernements peuvent  
promouvoir la transformation numérique

OCTOBRE 2019



## À PROPOS DU FPP

**Bonnes politiques. Meilleur Canada.** Le Forum des politiques publiques (FPP) rassemble différentes parties prenantes au processus d'élaboration des politiques. Il leur offre une tribune pour examiner des questions et apporter de nouveaux points de vue ainsi que de nouvelles idées dans des débats cruciaux sur les politiques. Nous croyons que l'élaboration de bonnes politiques est essentielle à la création d'un Canada meilleur – un pays cohésif, prospère et sûr. Nous y contribuons en :

- Menant des recherches sur des questions cruciales;
- Stimulant des dialogues sincères sur des sujets de recherche;
- Célébrant le travail de leaders exceptionnels.

Notre approche – appelée « de l'inclusion à la conclusion » – mobilise des interlocuteurs, connus ou non, qui nous aident à tirer des conclusions afin de cerner les obstacles à la réussite et de trouver des pistes de solutions.

Le FPP est un organisme de bienfaisance indépendant et non partisan qui compte parmi ses membres différents organismes privés, publics et à but non lucratif.

© 2019, Forum des politiques publiques

1400 – 130, rue Albert

Ottawa (Ontario) Canada K1P 5G4

613 238-7858

ISBN : 978-1-988886-77-0

[ppforum.ca](http://ppforum.ca)

[@ppforumca](https://www.instagram.com/ppforumca)

REMERCIEMENTS À NOTRE PARTENAIRE

# amazon web services institute

## AUTEURS

**Satyamoorthy Kabilan, Ph. D.**

Ancien vice-président, Politiques publiques, Forum des politiques publiques

## CONTRIBUTEURS

**Diana Del Bel Belluz**

Présidente, Risk Wise

**Nicole Foster**

Directrice des politiques publiques, Amazon Web Services (Canada)

**Katherine Feenan**

Responsable des politiques, Forum des politiques publiques

**Maysam Ali**

Responsable du contenu, AWS Institute

# TABLE DES MATIÈRES

Résumé .....	5
Introduction.....	7
Le gouvernement face au numérique : le risque du statu quo .....	8
1. Le risque des systèmes anciens.....	10
2. Le risque pour la cybersécurité.....	12
3. Le risque lié à la culture et aux personnes.....	13
4. Le risque de rupture de services.....	15
Conclusion .....	17
Annexe – Méthodologie.....	18

# RÉSUMÉ

Partout dans le monde, les gouvernements récoltent les fruits des technologies numériques, lesquels se traduisent par l'optimisation du rendement, la création de nouveaux services et l'amélioration de l'ouverture et de la transparence. Toutefois, l'adoption de la technologie se heurte parfois à l'aversion au risque et aux perceptions des dirigeants gouvernementaux. Les dirigeants ont tendance à se focaliser sur l'évaluation des coûts et des risques liés à l'adoption de nouveaux systèmes et mécanismes et ne tiennent pas toujours compte des risques associés au maintien du statu quo.

Le présent document examine les conséquences de l'incapacité à adopter les technologies numériques pour améliorer les services publics au Canada. Il a été éclairé par une série d'entrevues, un sondage et une table ronde avec de hauts fonctionnaires canadiens. L'analyse s'est également appuyée sur les connaissances de 16 dirigeants gouvernementaux, actuels et anciens, du Royaume-Uni, d'Écosse, de Nouvelle-Zélande, d'Australie, de Finlande, des États-Unis et du Canada pour comprendre le contexte mondial de cette question et trouver de nouvelles approches pour relever ce défi.

Le maintien du statu quo présente quatre grands risques :

- 1. Le risque lié aux systèmes anciens** découle de l'utilisation de technologies désuètes auxquelles les concepteurs ne fournissent parfois plus de soutien technique, dont l'entretien exige des compétences spéciales ou des dépenses considérables, ou qui créent des obstacles à l'intégration dans les nouvelles technologies. Ce risque comprend les répercussions de méthodes d'approvisionnement archaïques qui amènent les gouvernements à maintenir les systèmes anciens plutôt que de chercher de nouvelles technologies performantes. La prise en compte du risque lié aux systèmes anciens donne une image plus globale de ce que coûte le statu quo par rapport à la transformation numérique.
- 2. Le risque pour la cybersécurité** augmente avec l'utilisation de systèmes anciens en raison des vulnérabilités causées par l'incapacité à les sécuriser et l'absence de mises à jour. Lors de l'évaluation des risques liés à la transformation numérique, le remplacement des systèmes anciens doit être considéré comme une question de cybersécurité.
- 3. Le risque en ce qui a trait à la culture et aux personnes** est multiforme : premièrement, le fait d'être en retard sur les transformations numériques peut pousser les talents émergents vers un marché du travail plus compétitif et plus numérique. Deuxièmement, la culture organisationnelle peut avoir tendance à stagner, créant un obstacle considérable à la transformation numérique.
- 4. Le risque de rupture de services** augmente, car le fossé entre la prestation des services gouvernementaux et les attentes de la population s'élargit. Si le gouvernement ne tient pas compte des attentes, il risque de perdre son attrait, de causer de la frustration et d'éloigner les citoyens et citoyennes.

Les gouvernements doivent prendre conscience des risques liés au maintien du statu quo, et non seulement de ceux associés au changement et à la modernisation. Les stratégies définies pour faire face au risque du statu quo consistent à :

- 1. Tenir compte de l'entretien des systèmes anciens** lorsque la transformation numérique est envisagée. Cela devrait inclure le coût des compétences, le risque de ne plus comprendre le fonctionnement et d'assurer le soutien technique des systèmes anciens et l'accumulation de la dette technique dans ces systèmes. Cette analyse supplémentaire fournira un tableau beaucoup plus complet des décisions relatives à la transformation numérique, des économies de coûts et des mesures d'atténuation des risques qui pourraient être réalisées grâce à la transformation. L'examen des procédures d'approvisionnement désuètes permettra également de prendre en considération les possibilités numériques à long terme.
- 2. Envisager la nécessité de remplacer les systèmes anciens sous l'angle de la cybersécurité pour lui donner plus de poids.** La meilleure façon d'évaluer les répercussions possibles de la transformation numérique est de les comparer au risque potentiellement plus grand de problèmes de cybersécurité, comme une violation de données – et celui d'être exposé et blâmé publiquement.
- 3. Tenir compte du coût financier des risques pour la cybersécurité posés par les systèmes anciens.** Lorsqu'elles évaluent le coût global de la transformation numérique, les organisations victimes d'une violation de données doivent prendre en considération la perte de données, la perturbation des activités, les sanctions prévues par la réglementation et les autres facteurs. Cela fournit un tableau plus complet de l'analyse globale des risques nécessaire pour apporter une modification.
- 4. Utiliser la transformation numérique pour attirer et retenir les talents.** Le passage à une culture organisationnelle numérique et l'ouverture à la flexibilité, à l'innovation et à l'adoption rapide de la technologie peuvent réduire le risque de perdre ou de ne pas attirer du personnel qualifié. Dans un environnement où les secteurs privé et public se disputent les meilleurs employés, il est indispensable de comprendre comment la transformation numérique peut attirer les talents.
- 5. Tenir compte des risques liés à la pertinence du gouvernement et à l'engagement des citoyens et des citoyennes,** qui est maintenant un indicateur de rendement clé pour de nombreux gouvernements. Les gouvernements doivent améliorer la façon dont ils fournissent les services pour répondre aux besoins de la population. Résister à la transformation numérique risque de refréner cet engagement.

Le statu quo représente un risque important et devrait être un élément central du processus global d'évaluation des risques de toute initiative de transformation numérique.

# INTRODUCTION

La prolifération des technologies numériques dans l'économie a changé la façon dont les gens reçoivent les services et a perturbé de nombreux secteurs, notamment le commerce de détail, la finance et les transports. La numérisation a également transformé les citoyens et citoyennes en consommateurs avisés en matière de technologie, qui s'attendent à une prestation efficace des services gouvernementaux. Mais les gouvernements hésitent encore à accepter pleinement la transformation numérique. Bien que les risques qui y sont liés aient été largement explorés, le maintien du statu quo et ses risques inhérents importants n'ont pas encore été étudiés de façon aussi approfondie.

Pour le gouvernement, la transformation numérique peut prendre de nombreuses formes, allant de la prestation en ligne de services existants offerts à la population à l'accès libre aux données, en passant par l'interconnexion des ministères et la fourniture aux internautes d'une expérience homogène. Par ricochet, cela encourage le développement de services, nouveaux ou améliorés, qui peuvent fournir aux fonctionnaires les outils numériques dont ils ont besoin pour travailler plus efficacement. Partout dans le monde, les gouvernements ont répondu aux attentes changeantes des citoyens et citoyennes en adoptant un programme de transformation numérique.

## Le Canada stagne-t-il?

**En 2017, le Canada s'est classé 12<sup>e</sup> sur 60 pays selon l'Indice d'évolution numérique, mais 48<sup>e</sup> en ce qui concerne le développement numérique.**

De nombreux organismes gouvernementaux s'efforcent maintenant d'utiliser les technologies numériques pour offrir l'expérience efficace et conviviale que les citoyens et citoyennes exigent. L'Institute for Business in the Global Context de la Fletcher School de l'Université Tufts suit le développement numérique dans 60 pays depuis 2008. Il évalue les pays sur la base de 170 indicateurs pour attribuer une note sur l'Indice d'évolution numérique (IEN). Dans le classement le plus récent<sup>1</sup>, le Canada se trouve dans la catégorie « Pays stagnants », réservée aux nations les plus avancées sur le plan numérique, mais qui risquent de prendre du retard dans leur développement en raison de leur ralentissement.

Depuis cette évaluation, le gouvernement du Canada a élaboré une stratégie numérique<sup>2</sup> qui vise à améliorer et à moderniser la prestation des services par la transformation numérique. Toutefois, le présent document postule que l'aversion au risque enracinée chez les fonctionnaires canadiens<sup>3</sup> a créé un parti pris en faveur du maintien du statu quo plutôt que de l'adoption de nouvelles technologies<sup>4</sup>, et que la résistance a un coût.

<sup>1</sup> Chakravorti, B., et Chaturvedi, R.S. 2017. [Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World](#). The Fletcher School, Université Tufts.

<sup>2</sup> Gouvernement du Canada. 2018. [Plan stratégique des opérations numériques de 2018 à 2022](#).

<sup>3</sup> Bureau du vérificateur général du Canada. 2018. [Message du vérificateur général du Canada](#). Gouvernement du Canada.

<sup>4</sup> Aitken, K. 2018. [La gouvernance à l'ère numérique](#). Le Forum des politiques publiques.

## « Système ancien »

**Est défini au sens large comme un système d'information basé sur des technologies obsolètes qui est toujours indispensable pour les opérations quotidiennes.**

Oui, remplacer un système, avec toutes les technologies anciennes qui s'y rattachent, peut entraîner des défaillances massives. Il ne faut pas chercher plus loin que l'échec récent et très médiatisé du système de paye Phénix<sup>5</sup>, récemment mis en œuvre par le gouvernement du Canada. Le Bureau du vérificateur général du Canada a constaté que ce système est moins efficace et plus coûteux que celui qu'il a remplacé et que des milliers d'employés sont mal payés ou ne sont pas payés à temps. Cependant, des échecs qui défraient la chronique comme celui de Phénix peuvent exacerber les préjugés contre le changement, faisant paraître les résultats catastrophiques bien plus probables qu'ils ne le sont en réalité. Lorsque le souvenir des échecs l'emporte sur les avantages perçus du changement, cela diminue la propension au risque

et engendre un parti pris évident pour le statu quo.

Toutefois, le maintien du statu quo et le choix de ne pas adopter les nouvelles technologies comportent également des risques importants. Et bien que les défis liés à la transformation soient bien documentés, les risques associés au maintien du statu quo demeurent pour la plupart inexplorés<sup>6</sup>. La connaissance de ces risques peut jouer un rôle important dans le choix d'une organisation de procéder ou non à la transformation numérique.

Le présent document est éclairé par une série d'entrevues individuelles avec des cadres supérieurs clés des technologies de l'information (TI) au Canada et dans d'autres pays, dont la liste figure à l'annexe. Pour étudier l'expérience du Canada en matière de transformation numérique au niveau du personnel, un sondage a été mené auprès de professionnels des TI du gouvernement du Canada. De plus, le document est étayé par une table ronde organisée par le Forum des politiques publiques et l'Amazon Web Services Institute, qui a réuni de hauts dirigeants des secteurs public et privé pour discuter des risques et des possibilités liés à la modernisation. Grâce à ces entrevues, au sondage et à la recension des écrits récents, cette initiative explore quelques-uns des risques liés au maintien du statu quo dans ce domaine au sein du gouvernement au Canada. Des entrevues et des études de cas à l'échelle internationale ont été utilisées pour élargir le contexte et élaborer des stratégies pour lutter contre le statu quo.

## LE GOUVERNEMENT FACE AU NUMÉRIQUE : LE RISQUE DU STATU QUO

Des membres du gouvernement, actuels et anciens, interrogés, ont énuméré une foule d'obstacles à la transformation numérique. Citons notamment :

<sup>5</sup> Bureau du vérificateur général du Canada. 2018.. [Rapport 1 -- La création et le déploiement du système de paye Phénix](#)

<sup>6</sup> Davey, L. 2014. [The Status Quo is Risky, Too](#). Harvard Business Review.

- un paysage numérique en évolution rapide où il est difficile d'élaborer une stratégie efficace et où la nature, l'orientation et l'ampleur des changements potentiels de la technologie numérique évoluent de façon imprévisible<sup>7</sup>;
- une mauvaise compréhension de l'état numérique d'une organisation, de sorte qu'il est difficile de tracer une voie à suivre pour la transformation;
- des dirigeants focalisés sur l'élaboration de politiques plutôt que sur l'avancement de la transformation numérique;
- une orientation à court terme basée sur les exigences immédiates de réussite et les cycles électoraux.

Ces facteurs créent un environnement dans lequel les membres du gouvernement considèrent le maintien du statu quo numérique comme l'option la moins risquée. Bon nombre des membres de gouvernements étrangers interrogés ont indiqué que les fonctionnaires de leur pays avaient également ce parti pris pour le statu quo.

Au Canada, le parti pris pour le statu quo est renforcé par une forte aversion au risque et à l'échec, comme l'atteste une récente déclaration du vérificateur général :

« Un vaste groupe de personnel politique donne des conseils stratégiques aux ministres que les sous-ministres sont pourtant chargés de conseiller. Il est donc plus difficile pour les sous-ministres d'être entendus. Dès lors, il est plus facile pour eux de suivre simplement la volonté du ministre sans poser de questions, plutôt que de lui donner des avis courageux sur les embûches qui pourraient survenir et sur la manière de les éviter. C'est ainsi que les sous-ministres conservent la confiance de leur ministre et préservent le peu d'influence qu'ils ont.

Il ressort de cette dynamique une fonction publique docile qui tente d'éviter tout risque et erreur, ce qui est bien sûr impossible, de sorte qu'elle cherche plutôt à éviter de devoir assumer la responsabilité des erreurs qui surviennent.

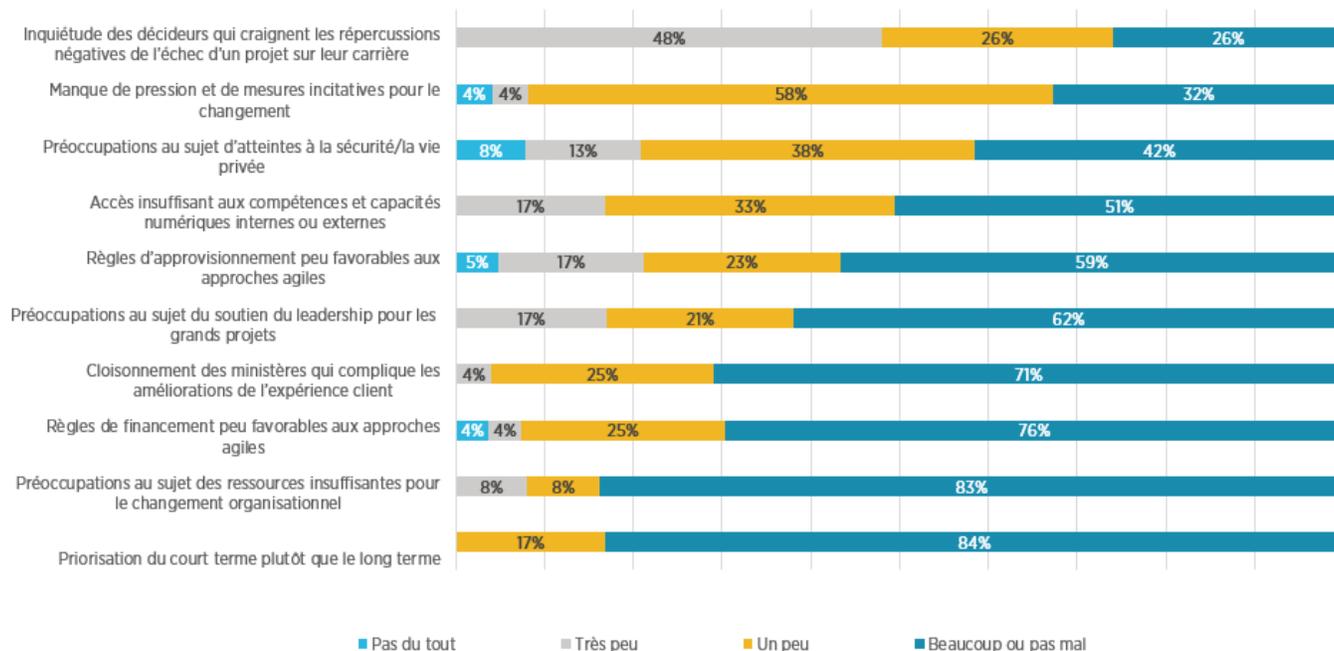
Dans cette culture, pour un fonctionnaire, il est souvent préférable de ne rien faire plutôt que d'agir puis d'échouer<sup>8</sup>. »

<sup>7</sup> Ce sentiment est étudié de plus près dans McKinsey & Company, 2019. [Navigating a World of Disruption](#).

<sup>8</sup> Bureau du vérificateur général du Canada. 2018. [Rapport du printemps présenté au Parlement du Canada Risque incompréhensible](#)

Toutefois, les répondants de notre sondage<sup>9</sup> montrent que plusieurs facteurs autres que la crainte de l'échec ont tendance à pousser les décideurs à maintenir le statu quo.

**Veillez évaluer les aspects suivants qui poussent actuellement les décideurs politiques de votre ministère ou de votre organisme à maintenir le statu quo et à éviter la transformation numérique**



Les risques bien documentés de la transformation numérique, associés à un certain nombre de facteurs structurels qui découragent le changement, font que les gouvernements tendent vers le statu quo. Cependant, les risques du statu quo ne sont pas aussi souvent abordés que ceux liés à l'adoption de la transformation<sup>10</sup>. Pour élargir cette conversation, nous avons cerné quatre risques clés auxquels font face les gouvernements qui choisissent le statu quo :

## 1. LE RISQUE DES SYSTÈMES ANCIENS

Les systèmes anciens peuvent être définis au sens large comme des systèmes d'information basés sur des technologies obsolètes qui sont toujours indispensables pour les opérations quotidiennes<sup>11</sup>. Les discussions avec des hauts dirigeants des TI du gouvernement et du secteur privé ont révélé que les systèmes anciens constituent un obstacle à la transformation numérique, à la modernisation et à l'adoption de nouvelles technologies innovantes. Au Royaume-Uni, 46 % des systèmes informatiques des collectivités locales

<sup>9</sup> Vingt-quatre personnes ont répondu au sondage, dont 42 % ont dit exercer un rôle de cadre supérieur dans la transformation numérique, alors que 17 % ont précisé qu'ils exerçaient une direction technique. Le text complet du questionnaire est disponible en ligne (veuillez consulter l'annexe pour l'hyperlien).

<sup>10</sup> Davey, L. 2014. [The Status Quo is Risky, Too](#). Harvard Business Review.

<sup>11</sup> Gartner IT Glossary. 2019. [Legacy application or system](#).

britanniques utilisent encore des logiciels datant des années 2000<sup>12</sup>. Dans de nombreux cas, le coût et la complexité de la modernisation de ces systèmes sont considérés comme un obstacle au changement. Des procédures d'approvisionnement désuètes influent également sur les décisions du gouvernement d'utiliser les systèmes existants plutôt que de chercher de nouvelles technologies habilitantes. Les personnes interrogées ont souligné la lourdeur des méthodes d'approvisionnement, qui dissuade les dirigeants des ministères d'envisager des solutions à long terme. Au lieu de cela, des solutions à court terme aux systèmes obsolètes semblent être une voie plus facile et plus rentable – mais le maintien en place de tels systèmes anciens entraîne des coûts importants, souvent négligés.

Selon un récent livre blanc de l'Association canadienne de la technologie de l'information (ACTI), l'utilisation continue des systèmes anciens obsolètes est également un problème au Canada<sup>13</sup>. L'ACTI estime que le gouvernement canadien dépense environ 12,5 milliards de dollars par année pour maintenir des systèmes informatiques désuets. L'entretien de ces systèmes anciens peut nécessiter des compétences et des connaissances spécialisées et, à mesure que les personnes qui participent à la construction et à l'entretien de ces systèmes changent d'activité ou même prennent leur retraite, la capacité de continuer à les entretenir s'amenuise rapidement. Il est de plus en plus difficile et coûteux de trouver des travailleurs qui connaissent et peuvent entretenir des technologies anciennes sur mesure. La diminution rapide du bassin de talents doit être considérée comme un coût et une vulnérabilité<sup>14</sup> pour l'ensemble du système.

Selon une estimation du consultant numérique Accenture, la dette technique du gouvernement des États-Unis – le coût de la mise à niveau des systèmes anciens qu'une organisation a accumulés au fil du temps – s'élève à environ 1,5 million de dollars par application<sup>15</sup>. En 2016, ce montant s'élevait à 7,5 milliards de dollars en matériel et logiciels en fin de vie, sans compter les systèmes obsolètes qui limitent déjà considérablement les opérations<sup>16</sup>. Ces coûts ne cessent d'augmenter.

Au Royaume-Uni, comme l'a indiqué une personne interrogée, le gouvernement utilise actuellement environ 900 systèmes d'information différents, et jusqu'à 800 d'entre eux sont considérés comme anciens. L'utilisation, la mise à jour et la réparation d'une technologie ancienne peuvent entraîner des problèmes supplémentaires liés à la sécurité, aux lois internationales ou aux exigences de conformité aux normes – comme le Règlement général sur la protection des données (RGPD) de l'Union européenne – et la capacité décroissante de ces systèmes à répondre aux besoins des utilisateurs.

Le maintien du statu quo par l'entremise de systèmes anciens devient de plus en plus coûteux. Les coûts de maintenance et d'exploitation des systèmes anciens du gouvernement des États-Unis représentaient 70 % du budget total des TI, soit 85,2 milliards de dollars, pour l'exercice 2018, contre 68 % pour l'exercice 2015<sup>17</sup>. En

---

<sup>12</sup> Frazzetto, A. 2018. [Rewrite or rebuild? 5 legacy system upgrade considerations](#). CIO.

<sup>13</sup> ACTI, 2019. [Developing a commercial first approach](#).

<sup>14</sup> Ibid.

<sup>15</sup> Accenture, 2018. [Decouple to Innovate](#).

<sup>16</sup> Miller, J. 2016. [Why \\$39,000 shows why the IT modernization effort matters so much](#). Federal News Network.

<sup>17</sup> Abel, R. 2019. [Looming retirement of legacy system custodians put global IT systems at risk](#). SC Magazine.

fait, la transformation numérique apparaît beaucoup moins coûteuse et moins risquée une fois que les coûts réels des systèmes anciens sont pris en compte.

## STRATÉGIE

### Prise en compte du coût de l'entretien des systèmes anciens

En envisageant la transformation numérique, il faut tenir compte des coûts et des risques liés à l'utilisation des systèmes anciens. Les facteurs à prendre en considération devraient inclure le coût des compétences, la diminution de la capacité de comprendre le fonctionnement et d'assurer le soutien technique des systèmes anciens, et l'accumulation de la dette technique dans ces systèmes. Cette analyse supplémentaire fournira un tableau beaucoup plus complet des choix de mise à niveau, des économies de coûts et des mesures d'atténuation des risques que permet la transformation numérique. L'examen des procédures d'approvisionnement désuètes permettra également d'envisager des possibilités numériques à long terme.

## 2. LE RISQUE POUR LA CYBERSÉCURITÉ

La sécurité est l'un des principaux défis posés par les systèmes anciens<sup>18</sup>. Une fois qu'une technologie est obsolète, il devient de plus en plus difficile de la protéger, ainsi que les données qu'elle contient, contre les menaces à la cybersécurité<sup>19</sup>. Un système ancien dans une architecture d'entreprise moderne et sécurisée ressemble à une porte d'entrée gardée alors que la porte arrière est déverrouillée. Au moment d'opter pour le remplacement d'un système ancien, il faut tenir compte du coût des brèches de cybersécurité.

La violation de données de l'Office of Personnel Management (OPM) des États-Unis en 2014 – l'une des plus importantes atteintes à la vie privée de l'histoire concernant les données personnelles d'employés du gouvernement des États-Unis – a été attribuée à l'utilisation de systèmes anciens qui ne permettaient pas le cryptage des données<sup>20</sup>. La violation a touché 21,5 millions<sup>21</sup> de personnes et a donné lieu à la passation d'un marché d'un montant de 133 millions de dollars pour la protection contre le vol d'identité<sup>22</sup>. Le coût de la

<sup>18</sup> DeBrusk, C., Mee, P., et Brandenburg, R. 2018. [The Marriott Data Breach](#). Oliver Wyman.

<sup>19</sup> Frazzetto, A. 2018. [Rewrite or rebuild? 5 legacy system upgrade considerations](#). CIO.

<sup>20</sup> Bisson, D. 2018. [Lagging Legacy Systems: How Federal Agencies Are Tackling Old IT](#). Tripwire.

<sup>21</sup> OPM Cybersecurity Resource Center, <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>

<sup>22</sup> OPM. 1<sup>er</sup> septembre 2019 [OPM, DoD Announce Identity Theft Protection and Credit Monitoring Contract](#). OPM News release.

surveillance du crédit à lui seul est passé à 416 millions de dollars au cours des années ultérieures et devrait augmenter à mesure que l'OPM continue d'offrir ce service aux personnes touchées par la violation.

De même, une faille dans un système ancien a causé une violation de données catastrophique chez l'opérateur de télécommunications britannique TalkTalk en 2015, entraînant le vol de coordonnées bancaires et de données personnelles de 157 000 clients, ainsi qu'une amende record de 400 000 £ imposée par le bureau du commissaire à l'information du Royaume-Uni<sup>23</sup>.

Des exemples abondent de systèmes et d'outils anciens ayant entraîné d'importantes atteintes à la protection des données, des problèmes de sécurité ou des conséquences juridiques. Le coût total moyen d'une seule violation s'élevant à 3,89 millions de dollars<sup>24</sup>, les risques et les coûts potentiels de l'entretien des systèmes anciens du point de vue de la cybersécurité ne cessent d'augmenter.

## STRATÉGIES

### Faire du remplacement des systèmes anciens une question de cybersécurité

**Inclure le volet cybersécurité dans la transformation numérique peut donner plus de poids à cette question. Il est plus probable d'accepter de relever le défi de la transformation numérique si on la compare au risque potentiellement plus grand des conséquences des problèmes de cybersécurité, comme la violation des données – et au risque d'être publiquement exposé et blâmé pour cela.**

### Tenir compte du coût financier des risques de cybersécurité posés par les systèmes anciens

**Bien qu'il soit difficile d'estimer le coût réel d'un incident de cybersécurité, les organisations concernées doivent prendre en compte le coût de la perte de données, de la perturbation des activités, des sanctions prévues par la réglementation et d'autres facteurs lorsqu'elles évaluent le coût global de la transformation numérique. Ce complément d'information fournit un tableau plus complet de l'analyse globale des risques liés à la transformation numérique.**

## 3. LE RISQUE LIÉ À LA CULTURE ET AUX PERSONNES

L'un des principaux mantras de la transformation numérique – répété à bien des égards par les personnes interrogées dans le cadre de cette étude – est qu'elle ne se limite pas à la technologie. La transformation numérique doit être holistique, englobant les personnes, les procédures et la culture. Comme l'a déclaré un

<sup>23</sup> Shephard, A. 2018. [« It's the legacy that get's you », warns ex-TalkTalk boss](#). ITPro.

<sup>24</sup> Ponemon Institute and IBM Security. 2018. [2018 Costs of a Data Breach Study: Global Overview](#).

dirigeant principal de l'information (DPI) : « La transformation numérique est un changement fondamental dans la façon d'administrer et de fournir des services. C'est donc une démarche à long terme et un processus culturel. Vous ne pouvez pas vous tromper de beaucoup si vous collaborez avec les gens dès le début. »

Le passage à une culture organisationnelle qui permet à la fois la transformation numérique et l'adoption rapide de la technologie est difficile à effectuer, ce qui est compréhensible. En fait, un programme sur trois de changement de culture organisationnelle échouent et seulement quelques-uns réussissent réellement<sup>25</sup>. La difficulté à traiter avec les personnes et les syndicats, ainsi que le taux d'échec élevé des programmes de changement de culture organisationnelle, créent une aversion au risque. Que les organisations choisissent ou non de s'engager dans la voie de la transformation numérique, il y a un parti pris inhérent en faveur du maintien de la culture organisationnelle actuelle.

Malheureusement, les cultures organisationnelles traditionnelles qui n'ont pas pleinement intégré la réalité numérique d'aujourd'hui comportent d'autres risques. Les travailleurs choisissent les emplois sur la base de la culture, des valeurs organisationnelles et des stratégies de recrutement innovantes<sup>26</sup>. Ils recherchent un environnement de travail activement ouvert à un monde numérique caractérisé par des changements et des mises à niveau réguliers. Le fait de posséder une culture numérique peut exercer un attrait sur les talents<sup>27</sup>, et avec la concurrence que se livrent les organisations pour attirer des employés dotés de compétences technologiques – qui ont tendance à être jeunes –, celles qui n'adoptent pas une culture numérique courent le risque de perdre des talents. Cette préoccupation a également été soulevée par les participants à la table ronde.

Le récent rapport publié par le FPP et l'AWS Institute, et intitulé « Développer la fonction publique canadienne pour le numérique », a mis en lumière le fait que l'environnement hiérarchique et la culture gouvernementale traditionnels ne sont pas attractifs pour de nombreux employés jeunes, surtout les femmes, qui sont avisés en matière de technologie<sup>28</sup>. Cette conclusion a été répétée par les personnes interrogées dans le cadre de ce projet. En fait, comme l'indique le tableau ci-dessus, lorsqu'ils ont été interrogés sur les aspects qui influencent les décideurs à maintenir le statu quo et à éviter la transformation numérique, 83 % des répondants ont indiqué qu'ils étaient préoccupés par l'insuffisance des ressources nécessaires pour le changement organisationnel. La moitié d'entre eux a déclaré que l'accès insuffisant aux compétences et capacités numériques internes ou externes était un facteur déterminant.

Les gouvernements doivent offrir aux employés, actuels et nouveaux, la possibilité d'améliorer leurs compétences tout en mettant à niveau continuellement leur technologie pour soutenir un milieu de travail en évolution. Le maintien d'une culture organisationnelle qui ne tient pas compte des changements

---

<sup>25</sup> Lyons, R. 2017. [Three Reasons Why Culture Efforts Fail](#). Forbes.

<sup>26</sup> [Nuage de talents](#), la plateforme expérimentale du gouvernement du Canada, offre une nouvelle vision du recrutement et des offres d'emploi dans le secteur public; toutefois, une plus grande attention de la part des ministères et un financement accru seront nécessaires pour son succès.

<sup>27</sup> Hemerling, J.; Kilmann, J.; Danoesastro, M.; Stutts, L.; et Ahern, C. 2018. [It's Not a Digital Transformation without a Digital Culture](#). BCG.

<sup>28</sup> Cukier, W. 2019. [Développer la fonction publique canadienne pour le numérique](#). Le Forum des politiques publiques.

technologiques risque d'éloigner les compétences dont les organisations d'aujourd'hui ont le plus besoin. Avoir des employés avisés en matière de technologie comporte l'avantage supplémentaire qu'ils deviennent des défenseurs du changement numérique et de l'adoption de nouvelles technologies.

## STRATÉGIE

### La transformation numérique aide à attirer et à retenir les talents

**Le passage à une culture organisationnelle numérique ouverte à la flexibilité, à l'innovation et à l'adoption rapide de la technologie peut réduire le risque de l'incapacité à attirer des travailleurs qualifiés. Dans un environnement où les secteurs privé et public se disputent les meilleurs employés, il est indispensable de comprendre comment la transformation numérique peut attirer des talents.**

## 4. LE RISQUE DE RUPTURE DE SERVICES

Un principe clé se dégage partout dans le monde : les citoyens et citoyennes veulent bénéficier du même niveau de service et de commodité dans le secteur public que dans les entreprises privées<sup>29</sup>. Ce principe a été l'un des moteurs du programme de transformation numérique de nombreux gouvernements, dont celui du Canada<sup>30</sup>. Dans le secteur privé, l'incapacité de répondre à l'évolution des besoins et des demandes des clients peut entraîner une perte d'activité, étant donné que les concurrents s'efforcent de proposer une meilleure solution de rechange. Au cours de la dernière décennie, le fait de ne pas répondre aux attentes des clients a été un facteur déterminant dans la perturbation numérique mondiale de nombreuses entreprises.

Si les gouvernements ne fournissent pas les services correspondant aux attentes, et ne simplifient pas les procédures à l'aide de la technologie, d'autres organisations sont susceptibles d'intervenir. Ainsi, les gouvernements risquent de devenir moins pertinents<sup>31</sup> et, en fin de compte, moins fiables si les citoyens et citoyennes se sentent obligés de chercher d'autres sources pour mieux répondre à leurs besoins dans un environnement numérique. Comme l'a déclaré Scott Brison, ancien président du Conseil du Trésor et ministre du Gouvernement numérique : « Aujourd'hui plus que jamais, les entreprises et les gouvernements doivent comprendre leur principal objectif. Sinon, ils perdront toute pertinence avant de s'en rendre compte<sup>32</sup>. » En fin de compte, « nous ne pouvons pas être un gouvernement Blockbuster au service d'une population Netflix<sup>33</sup>. »

<sup>29</sup> Bertrand, A. 2019. [How does digital government become better government?](#) EY.

<sup>30</sup> Secrétariat du Conseil du Trésor. 2019. [Plan stratégique des opérations numériques de 2018 à 2022](#). Gouvernement du Canada.

<sup>31</sup> May, K. 2017. [Government relevance at stake in digital age](#). iPolitics.

<sup>32</sup> May, K. 2018. [Driving digital transformation of government. This time they mean it](#). iPolitics.

<sup>33</sup> Ibid.

Bien que les risques liés à la transformation numérique puissent empêcher les ministères d'évoluer, il leur faut trouver un équilibre entre ce risque et celui de perdre de leur pertinence et la confiance de la population. Les personnes interrogées ont souligné l'importance de mettre l'accent sur la prestation attendue aujourd'hui par les consommateurs : les services de base doivent être fournis de façon numériquement transparente dans tous les ministères. Les services sont actuellement offerts aux citoyens et citoyennes de manière fragmentée, dans divers points de contact, souvent dans des lieux différents où ils doivent fournir les mêmes renseignements à plusieurs reprises par exemple, après la naissance d'un enfant, lors d'un déménagement ou au moment du décès d'un être cher. Le fait d'offrir des services faciles d'accès et homogènes mènera à une interaction plus positive avec le gouvernement. Des solutions technologiques pourraient être utilisées pour permettre une approche en une seule étape qui achemine automatiquement l'information à plusieurs ministères de façon homogène plutôt que d'exiger que les citoyens et citoyennes fournissent la même information à plusieurs ministères.

## **STRATÉGIE**

### **Tenir compte des risques pour la pertinence du gouvernement et l'engagement des citoyens et citoyennes**

**L'engagement des citoyens et citoyennes est devenu un indicateur de rendement clé pour de nombreux gouvernements. Ces derniers doivent se préoccuper de leur propre pertinence et examiner régulièrement la façon dont ils fournissent leurs services. Résister à la transformation numérique risque de diminuer l'engagement des citoyens et citoyennes. Les gouvernements devraient tenir compte de ce résultat lorsqu'ils soupèsent les risques liés au maintien du statu quo.**

# CONCLUSION

La transformation numérique présente tout un éventail de défis, en particulier pour les gouvernements. Le gouvernement du Canada s'est focalisé sur la transformation numérique, mais nos recherches ont montré qu'un certain nombre d'obstacles demeurent. Bien que l'accent ait été mis sur les risques liés à l'adoption de la transformation numérique, le maintien du statu quo est beaucoup plus risqué et, au bout du compte, plus coûteux à long terme. La prise en compte des risques du statu quo dans le cadre de l'évaluation de la transformation numérique, particulièrement dans les quatre aspects que nous avons décrits, donnera une vision plus réaliste du risque global lié au changement numérique.

Les risques importants posés par le maintien du statu quo – notamment l'utilisation de systèmes anciens, l'augmentation des vulnérabilités en matière de cybersécurité, les obstacles à l'attrait des talents numériques, les défaillances potentielles des services et le désintérêt dû à l'absence de prestation de services numériques – illustrent pourquoi les dirigeants gouvernementaux doivent revoir leur perception des risques lorsqu'ils envisagent la transformation numérique. Les leçons tirées de l'expérience des gouvernements du monde entier montrent qu'en fin de compte, le changement numérique est le choix le moins risqué.

# ANNEXE – MÉTHODOLOGIE

## TABLE RONDE

La table ronde s'est tenue le 30 janvier 2019. Parmi les participants figuraient des hauts décideurs politiques, des universitaires et des dirigeants du secteur privé.

## ENTREVUES

Les entrevues ont été menées entre fin janvier et mi-février 2019. Pour protéger la confidentialité, les noms des personnes interrogées n'ont pas été divulgués. Toutefois, elles représentent les organisations suivantes :

### Participation à l'échelle internationale :

- Gouvernement écossais
- Ministère de la Justice du Royaume-Uni
- Ark (organisme de bienfaisance voué à l'éducation et basé au Royaume-Uni)
- Gouvernement de la Nouvelle-Zélande
- Gouvernement de l'Australie
- Ministère des Finances, Finlande
- Services des douanes et de l'immigration des États-Unis

### Participation à l'échelle du Canada :

- Banque du Canada
- Secrétariat du Conseil du Trésor
- Centre pour l'Innovation des données du gouvernement provincial de la C.-B.
- Inforoute Santé du Canada
- Services partagés Canada
- Transports Canada
- Agriculture et Agroalimentaire Canada
- Société canadienne d'hypothèques et de logement

## SONDAGE

Le sondage a été réalisé sur le terrain du 6 au 23 mars 2019. Des 176 personnes ayant reçu le questionnaire, 24 l'ont rempli en entier. Les personnes interrogées étaient issues d'un éventail de ministères et d'organismes gouvernementaux fédérales, provinciales, et internationales. Le sondage a été effectué en anglais seulement.

Pour lire le questionnaire au complet, veuillez consulter [ppforum.ca/fr/publications/statu-quo-numerique](http://ppforum.ca/fr/publications/statu-quo-numerique).



**FORUM DES  
POLITIQUES  
PUBLIQUES**