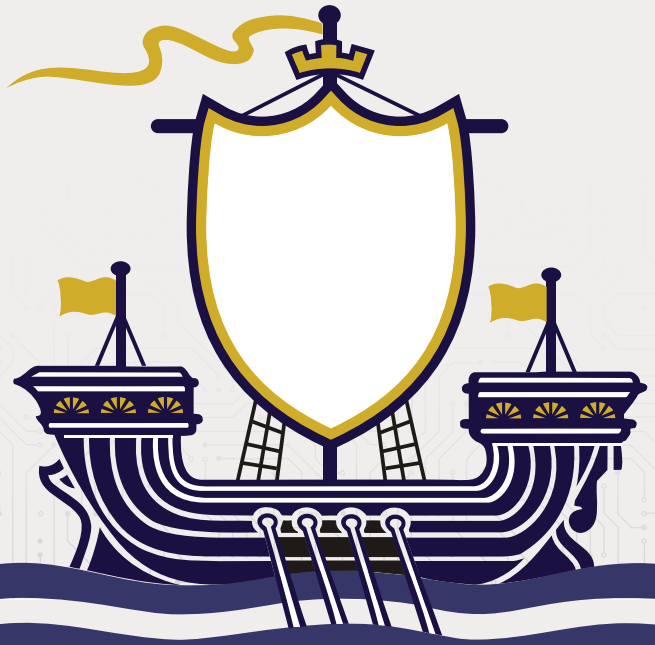
À la recherche des talents cachés

L'EXPÉRIENCE ET L'EXPERTISE DE LA COMMUNAUTÉ DE CYBERSÉCURITÉ DU NOUVEAU-BRUNSWICK



ICTC CTIC

Recherche par le Conseil des technologies
de l'information et des communications

Ce projet a été financé par le ministère de
l'Éducation postsecondaire, de la Formation
et du Travail du Nouveau-Brunswick

Préface

En tant que centre national d'expertise sans but lucratif, le CTIC cherche à renforcer l'avantage numérique du Canada dans l'économie mondiale. Grâce à des recherches de confiance, à des conseils stratégiques pratiques et à des programmes créatifs de renforcement des capacités, le CTIC favorise des industries canadiennes novatrices et concurrentielles à l'échelle mondiale, habilitées par des talents numériques novateurs et diversifiés. En partenariat avec un vaste réseau de chefs de file de l'industrie, de partenaires universitaires et de décideurs politiques de partout au Canada, le CTIC favorise une économie numérique inclusive et concurrentielle à l'échelle internationale depuis plus de 25 ans.

Pour citer ce rapport:

Herron, C., Rice, F., Snider, N. (Avril 2020). À la recherche des talents cachés : L'expérience et l'expertise de la communauté de cybersécurité du Nouveau-Brunswick. Conseil des technologies de l'information et des communications (CTIC). Ottawa, Canada.

Recherche et rédaction par Nathan Snider (gestionnaire, Politiques et sensibilisation), Faun Rice (analyste de la recherche et des politiques), et Chris Herron (analyste subalterne de la recherche) avec le généreux soutien d'Arun Sharvirala (scientifique des données), de Rob Davidson (gestionnaire, Analyse des données et recherche), d'Olivia Lin (analyste subalterne des données), et de l'équipe des politiques et de la recherche du CTIC.

Résumé

Le rapport À la recherche des talents cachés : L'expérience et l'expertise de la communauté de cybersécurité du Nouveau-Brunswick a pour but d'évaluer le type de demande pour du personnel en cybersécurité et son ampleur dans la province du Nouveau-Brunswick, une plaque tournante en cybersécurité reconnue au Canada. À cette fin, la présente étude utilise des données provenant d'un sondage mené auprès d'employeurs, d'entrevues réalisées auprès d'employeurs, d'organismes de perfectionnement de la main-d'œuvre et d'établissements d'enseignement. Des données tirées de sites d'emplois et des données secondaires approfondies fournies par Statistique Canada et d'autres sources y sont également présentées. En utilisant le cadre de la National Initiative for Cybersecurity Education (NICE) (un système de classification internationale de la main-d'œuvre en cybersécurité) pour comparer les différentes sources de données guidant la présente recherche, l'étude conclut que la demande pour des talents en cybersécurité au Nouveau-Brunswick varie selon le type de rôle et son degré de spécialisation. Les emplois qui exigent davantage d'expérience, comme la conception et la supervision de programmes de cybersécurité, sont beaucoup plus recherchés au Nouveau-Brunswick que les rôles qui pourraient être occupés par des candidats de premier échelon. Une analyse des compétences recherchées vient renforcer cette conclusion. La pénurie de *professionnels qualifiés et expérimentés* est un problème complexe à résoudre qui dépend d'une compréhension globale de l'écosystème de cybersécurité et des parcours professionnels. Par conséquent, la présente étude examine aussi *l'approvisionnement* de talents en cybersécurité, y compris les établissements d'enseignement et les données démographiques de la main-d'œuvre. Le rapport conclut en recensant plusieurs possibilités constructives de combler l'écart entre la demande et l'approvisionnement en cybersécurité au Nouveau-Brunswick.

La présente étude s'est conclue immédiatement avant l'explosion de cas de la COVID-19 au Canada, alors que les outils de recherche primaires ont tous pris fin le 1er février 2020. Par conséquent, les statistiques et les figures de ce rapport se fondent sur la croissance stable observée au sein de l'économie canadienne avant la crise de la COVID-19. La demande de main-d'œuvre subira probablement des répercussions défavorables à court terme (2020), quoiqu'elle devrait revenir à la normale en 2021 étant donné l'importance toujours actuelle du secteur de la cybersécurité. Le CTIC compte poursuivre des études de suivi et publiera, à l'automne 2020, un complément au présent rapport sur l'impact de la COVID-19.

Termes clés : Cybersécurité, recherche sur le marché du travail, National Initiative for Cybersecurity Education (NICE), Nouveau-Brunswick, perfectionnement de la main-d'œuvre

Remerciements

Le CTIC tient à remercier les personnes et les organismes qui ont offert leur temps et leur expertise en appuyant ou contribuant à la présente étude, notamment :

Paul Archer : Directeur de la sécurité, Kognitiv Spark

Agence de promotion économique du Canada atlantique

Stanley Barnaby : Directeur principal, Initiative conjointe de développement économique

Andrew Brewer : Président, CMS Consulting, Inc.

Shannon Brittany-Pollock : Stratège de la main-d'œuvre, CyberNB Inc.

Bulletproof

Kathryn Cameron : Chef de l'exploitation , Beauceron Security Inc.

Ian Daly : Coordonnateur de projets en TI, Initiative conjointe de développement économique; cofondateur et président, Kinap Solutions

Dillon Donahue : Spécialiste des cadres de formation, CyberNB Inc.

Harrison Duffley : Formateur coordonnateur, Technologies de l'information et cybersécurité, Collège communautaire (anglophone) du Nouveau-Brunswick

Mohamed Elghazouly : Chef de la cybersécurité et de la protection de la vie privée

Faruk Ener : Agent de développement des entreprises, Institut canadien sur la cybersécurité

Anthony English : Vice-président et responsable principal de la sécurité de l'information, Mariner Innovations

Gerry Fairweather : Sous-ministre adjoint et dirigeant principal de l'information, gouvernement du Nouveau-Brunswick : Finances et Conseil du Trésor

Sarah Corey Hollohan : Directrice, Ignite Fredericton

Susan Holt : Vice-présidente de la stratégie, Professional Quality Assurance Ltd.

Daniel Hoyles : Analyste des investissements, Fondation de l'innovation du Nouveau-Brunswick

Andrew Jefferies : Cadre-conseil en cybersécurité, Deloitte Canada

Richard Jones : Entrepreneur en résidence, Propel ICT Inc.

Chris Kantor : Directeur de campus, Eastern College

Jessica Kennedy : Gestionnaire de programme, Services des talents, Venn Innovation

Chris Lincoln : Directeur principal, Pratiques de sécurité, Bell Canada

Andrew Lockhart : Spécialiste du développement économique, Ignite Fredericton

Ian MacKinnon : Chef en matière de sécurité et de protection de la vie privée, Cirrus9

Jean-Marie Pelletier : Gestionnaire, Partenariats autochtones (éducation continue), Collège communautaire (francophone) du Nouveau-Brunswick

Adam Mosher : Fondateur et PDG, Global Intelligence Inc.

Frank Post : Directeur principal, Difenda

Jamie Rees : Chef de la sécurité de l'information d'entreprise, Travail sécuritaire NB

Laura Richard, Ph. D. : Directrice de la recherche, Fondation de l'innovation du Nouveau-Brunswick

Krista Ross : PDG, Chambre de commerce de Fredericton

Larry Shaw : PDG, Knowledge Park

Cathy Simpson : PDG, TechImpact

Paul Van Iderstine : CPA, CA, CISSP, GSEC, GCCC

Table des matières

Résumé

Aux côtés de nos partenaires internationaux, la demande du Canada pour des talents en cybersécurité continue d'augmenter. Pour chaque nouveau produit novateur de cybersécurité qui entre sur le marché, les pionniers qui mènent la marche en arrière-scène représentent un ensemble de plus en plus diversifié et spécialisé de compétences techniques. De plus, les établissements bien établis et les secteurs comme les finances, les services publics et les soins de santé nécessitent de plus en plus du personnel interne en cybersécurité pour les aider à se protéger contre les cyberattaques. Au Canada et ailleurs dans le monde, les employeurs envoient le message clair voulant qu'il soit difficile de trouver ces talents qualifiés, et c'est également le cas dans la province du Nouveau-Brunswick, l'une des plaques tournantes indéniables du Canada en matière de cybersécurité. Grâce à sa saine industrie de la cybersécurité, la province connaît une forte demande pour des recrues talentueuses, surtout celles possédant des compétences poussées et une riche expérience.

La demande de personnel en cybersécurité peut être mesurée de différentes façons, et la présente étude fournit un aperçu des différents paramètres permettant d'examiner et de comparer la demande en cybersécurité, autant au Nouveau-Brunswick que dans le reste du Canada, et entre les différents types d'emplois dans le domaine. En examinant plus largement les professions, il est évident que les rôles liés à la cybersécurité enregistrent des taux de chômage beaucoup plus faibles que d'autres rôles dans le secteur des technologies de l'information et des communications (TIC), tant au Nouveau Brunswick qu'au Canada dans son ensemble. Or, environ les deux tiers (67 %) des représentants de l'industrie de la cybersécurité du Nouveau-Brunswick interrogés dans le cadre de la présente étude chercheront à élargir leur bassin de main-d'œuvre en cybersécurité au cours de la prochaine année, et l'activité enregistrée sur les sites d'affichage d'emploi démontre un volume élevé de postes à pourvoir par rapport à la population de la province.

En utilisant le cadre de la National Initiative for Cybersecurity Education (NICE) (un système de classification internationale de la main-d'œuvre en cybersécurité) pour comparer les différentes sources de données guidant la présente étude, il est clair que la demande varie selon le type de rôle et son degré de spécialisation. Les catégories du cadre NICE exigeant un peu plus d'expérience, comme « Sécuriser l'approvisionnement » et « Encadrer et régir », sont plus recherchées au Nouveau-Brunswick que les rôles qui pourraient être dotés par des candidats de premier échelon. Cependant, ces professionnels qualifiés et expérimentés peuvent être difficiles à trouver : seulement environ un tiers des offres d'emploi du Nouveau-Brunswick dans ces catégories sont dotés en moins d'un mois, et elles exigent en moyenne au moins 6,7 années d'expérience.

Une analyse plus approfondie des compétences que recherchent les employeurs, ainsi que des obstacles qu'ils rencontrent en matière d'embauche, jette un peu plus de lumière sur cette tendance. Bien que l'embauche de talents qualifiés soit la principale difficulté que rencontrent les employeurs, la situation se complique en raison d'autres considérations comme les salaires élevés en cybersécurité et l'absence de parcours professionnel clair pour les nouveaux diplômés. Parmi les employeurs interrogés, seulement 1 sur 10 (11 %) estimait que le Nouveau Brunswick souffrait d'une pénurie de candidats en cybersécurité : par conséquent, les difficultés associées à l'embauche vont bien au-delà du simple approvisionnement brut.

En effet, l'approvisionnement provincial de diplômés en cybersécurité de premier échelon augmente alors que les collèges et les universités créent et améliorent rapidement leurs programmes ciblés, et la présente étude propose également un aperçu du nombre et de la variété de programmes en cybersécurité de la province. Tout comme il existe une rareté de rôles de mi-carrière, il y a aussi un manque de diversité dans la communauté de cybersécurité du Nouveau-Brunswick. Dans la présente étude, 28 % des employeurs interrogés ont indiqué que leur main-d'œuvre en cybersécurité était entièrement composée d'hommes de race blanche, et un peu plus de la moitié (52 %) précisaient qu'aucune femme n'occupait de rôle en cybersécurité.

La pénurie de professionnels qualifiés et expérimentés est un problème complexe à résoudre qui dépend d'une compréhension globale de l'écosystème de cybersécurité et des parcours professionnels. Néanmoins, la présente étude recense plusieurs possibilités constructives, comme un nombre accru d'occasions d'apprentissage intégré au travail et l'officialisation de parcours professionnels clairs pour les nouveaux diplômés. Tandis que l'industrie de la cybersécurité du Nouveau-Brunswick continue d'acquérir une renommée internationale, son écosystème bien réseauté et collaboratif est mûr pour une expansion continue. En tenant compte de certains ajustements et considérations cruciaux, la province peut assurément continuer de jouer dans la cour des grands dans le domaine de la cybersécurité à l'échelle nationale et mondiale.

Introduction

La cybercriminalité est un problème de plus en plus important pour le Canada et le reste du monde. Alors que des organisations partout au Canada commencent à adopter l'infonuagique, des appareils de l'Internet des objets et des systèmes numériques plus intégrés, la vulnérabilité du pays en matière de cybercriminalité augmente aussi. Les cyberattaques incluent les attaques de déni de service (le pirate bloque un système de TI, possiblement pour demander une rançon), l'hameçonnage (un message amenant des utilisateurs à fournir des renseignements personnels ou d'autres informations) et les logiciels malveillants (logiciels installés sur l'ordinateur d'un utilisateur sans son consentement). Les menaces connues comme l'atteinte à la protection des données ont des répercussions plus larges : plus les entreprises recueillent de données, plus elles sont vulnérables aux attaques. Les nouvelles technologies comme les dispositifs intelligents portables, les véhicules autonomes, l'infrastructure interconnectée et intelligente, l'infonuagique, l'automatisation, l'intelligence artificielle et les maliciels « sur commande » sont quelques-unes des nouvelles tendances suscitant des préoccupations croissantes dans le secteur de la cybersécurité[1].

Comprendre la cybersécurité

La cybersécurité peut être généralement définie comme la pratique consistant à se protéger contre des cyberattaques[2], qu'il s'agisse d'un particulier ou d'une organisation. La cybersécurité peut toucher la sécurité des réseaux, des systèmes et des programmes, la formation de membres du personnel pour les sensibiliser à la cybersécurité, ou l'élaboration d'un plan d'intervention en cas d'incidents. À ce titre, les entreprises du secteur de la cybersécurité subissent des pressions pour étendre leurs activités et innover alors que la cybercriminalité prend de l'ampleur et se complexifie.

En 2017, un peu plus du cinquième (21 %) de toutes les entreprises canadiennes de toutes les tailles[3] avaient été touchées par un incident de cybersécurité[4], et le Canada se classait au troisième rang mondial quant au nombre d'atteintes à la protection des données, après les États-Unis et le Royaume Uni[5]. De plus, l'Autorité canadienne pour les enregistrements Internet (ACEI) a signalé en 2018 que 4 PME canadiennes sur 10 avaient été victimes d'hameçonnage et de cyberattaques : environ un tiers d'entre elles avaient été visées par des chevaux de Troie et des logiciels espions, tandis que 27 % avaient été attaquées par des rançongiciels[6]. Alors que les attaques sont de plus en plus fréquentes et perfectionnées partout dans le monde, le besoin de talents qualifiés et réactifs. Dans une étude internationale réalisée en 2017, 66 % des entreprises du secteur de la sécurité de l'information ont indiqué qu'elles ne disposent pas de suffisamment de personnel pour traiter de ces menaces croissantes[7].

[1]Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017 : https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf, p. 2; Deloitte et Toronto Financial Services Alliance. The changing faces of cybersecurity: Closing the cyber risk gap, 2018 : https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF, p. 5.
[2]Cisco. « What Is Cybersecurity? » (sans date) : https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.
[3]En 2012, le ministère de la Sécurité publique et de la Protection civile a indiqué que les entreprises de moins de 250 employés faisaient partie du plus important secteur de croissance pour des cyberattaques ciblées. De plus, en 2012, 69 % des entreprises canadiennes interrogées comptant moins de 500 employés ont signalé une cyberattaque, causant des pertes moyennes de 15 000 $ par attaque. Le même rapport proposait d'élaborer des politiques internes, de former un employé à l'interne qui sera responsable de la cybersécurité, et de consulter des professionnels de la cybersécurité à l'externe au besoin. (Ministère de la Sécurité publique et de la Protection civile, Guide Pensez cybersécurité pour les petites et moyennes entreprises : https://www.pensezcybersecurite.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-fr.aspx)
[4]Statistique Canada. L'incident du cybercrime sur les entreprises canadiennes, 2017 : https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-fra.htm.
[5]Symantec Corporation. « Internet Security Threat Report », 2017 : https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf, p. 50.
[6]Autorité canadienne pour les enregistrements Internet (ACEI). Sondage sur la cybersécurité, automne 2018 : https://www.cira.ca/fr/resources/cybersecurite/rapport/2018-sondage-sur-la-cybersecurite.
[7]Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, 2017, p. 2.

Les professionnels de la cybersécurité sont responsables de protéger les organisations et les particuliers contre les cyberattaques. Les personnes qui possèdent les compétences pour créer, exploiter et maintenir des systèmes sécurisés tout en répondant aux menaces sont très recherchées, non seulement au Canada, mais dans l'ensemble des États-Unis et à l'échelle mondiale. La présente étude porte sur la demande de personnel en cybersécurité au Nouveau-Brunswick en particulier, plaçant la province dans un contexte international et national élargi.

Cybersécurité dans la province du Nouveau-Brunswick

Au Canada, la province du Nouveau-Brunswick est un important centre d'activités en cybersécurité, et la ville de Fredericton en particulier a été identifiée comme l'un des sept carrefours académiques en cybersécurité du pays[8]. L'Institut canadien sur la cybersécurité, une grappe de recherche qui inclut des unités de formation en cybersécurité ainsi que de développement entrepreneurial et académique, fait partie de l'Université du Nouveau-Brunswick à Fredericton[9]. En outre, Opportunités Nouveau-Brunswick et sa filiale CyberNB ont réalisé d'importants investissements dans la province pour subventionner des organisations génératrices d'emplois comme le Centre national d'innovation pour la cybersécurité[10] des Laboratoires Nucléaires Canadiens et le centre de cybersécurité[11] de Siemens. Le financement du gouvernement et d'investisseurs locaux (comme Ignite Fredericton, la Fondation de l'innovation du Nouveau-Brunswick et la Technology Venture Corporation) complète l'expertise académique de la province, en faisant un endroit idéal pour lancer des entreprises en cybersécurité[12].

Dans le cadre de la présente étude, le CTIC a discuté avec des représentants de l'industrie dans l'ensemble de la province qui ont commenté l'écosystème de cybersécurité unique et complexe du Nouveau-Brunswick[13]. Plusieurs des thèmes relevés par les personnes interrogées offrent un important contexte à l'orientation du rapport sur l'offre et la demande en cybersécurité.

Des relations solides entre le milieu universitaire et le secteur privé favorisent souvent un développement économique sain, et au Nouveau-Brunswick, ces relations sont perceptibles sur de nombreux plans.

Les universités travaillent directement sur des projets novateurs de recherche et développement, les collèges collaborent avec l'industrie dans le cadre des comités consultatifs de programmes pour s'assurer que ces derniers demeurent novateurs, et l'industrie a établi un lien direct avec les écoles primaires et secondaires pour offrir des occasions de mentorat aux jeunes. Plusieurs caractéristiques propres à la province s'harmonisent pour créer ces liens, notamment sa taille.

[8]Deloitte et Toronto Financial Services Alliance. The changing faces of cybersecurity: Closing the cyber risk gap, 2018, p. 15.
[9]Institut canadien sur la cybersécurité. « About the Canadian Institute for Cybersecurity ». Université du Nouveau-Brunswick, consulté le 22 mai 2019 : https://www.unb.ca/cic/about/index.html.
[10]« New National Innovation Centre for Cybersecurity opens in New Brunswick », DCN News Services, 1er juin 2018 : https://canada.constructconnect.com/dcn/news/projects/2018/06/new-national-innovation-centre-cybersecurity-opens-new-brunswick.
[11]« Siemens to open cybersecurity centre in Fredericton, create up to 60 jobs », CBC News, 30 mai 2018 : https://www.cbc.ca/news/canada/new-brunswick/siemens-cybersecurity-centre-fredericton-jobs-1.4684636.
[12]« Why New Brunswick is Canada's Cybersecurity Hub », Media Planet Industry and Business, septembre 2017 : http://www.industryandbusiness.ca/insight/why-new-brunswick-is-canadas-cybersecurity-hub.
[13]Les 16 personnes interrogées lors des entrevues incluaient des intervenants de l'industrie, du gouvernement et d'organismes sans but lucratif, et les rôles les plus fréquents étaient les responsables principaux de la sécurité de l'information, les dirigeants principaux de la technologie, les chefs en matière de sécurité, et les gestionnaires de talents.

Puisque l'industrie prend de l'ampleur, le Nouveau-Brunswick attire des entreprises très reconnues. Il existe un lien étroit rarement observé entre le milieu de l'éducation, l'industrie et le gouvernement. Les liens avec les représentants ministériels et les autres décideurs politiques sont plus faciles à établir que dans les centres urbains.

- Dillon Donahue, CyberNB

Comme l'a expliqué une autre des personnes interrogées, le Nouveau-Brunswick, en tenant compte dès le début des aspects de la cybersécurité (notamment des investissements provinciaux dans les infrastructures pertinentes dès le début des années 1990)[14], a permis aux initiatives de politique publique d'évoluer en même temps que l'industrie.

D'autres personnes interrogées laissaient entendre que la capacité de la province de venir à la table pour rencontrer les joueurs de l'industrie afin d'assurer une planification coordonnée a été déterminante pour son succès rapide.

Les investissements stratégiques des gouvernements provinciaux et fédéral ont permis de créer une solide fondation pour l'industrie. Toutefois, l'industrie a manifesté un engagement clair à définir les politiques de façon proactive dans la mesure du possible. Dans l'ensemble, les personnes interrogées estimaient que les joueurs de l'industrie partageaient un fort sentiment de soutien et d'encouragement pour une croissance continue, autant dans le secteur privé que le secteur public.

Lorsqu'il est question des menaces pour l'industrie de la cybersécurité du Nouveau-Brunswick, l'industrie de la province a un avantage sur les grandes régions métropolitaines comme Toronto et Vancouver : elle ne pille pas les talents en cybersécurité. Puisqu'il existe moins d'industries concurrentes dans la province, les professionnels de la cybersécurité tendent à collaborer davantage.

– Paul Van Inderstine, CPA, CA, CISSP, GSEC, GCCC

[14] *Kritsonis, Ted. Media Planet. « Fredericton, NB – a National Leader in Cyber Security », 2017 : http://www.industryandbusiness.ca/development-and-innovation/fredericton-nb-a-national-leader-in-cyber-security*

Les répondants ont également parlé d'un esprit communautaire profond parmi leurs pairs, mentionnant souvent d'autres organisations pour leurs inestimables contributions à l'écosystème de cybersécurité. Près des trois quarts des répondants ont explicitement mentionné les efforts fructueux pour perfectionner aussi la main-d'œuvre (déployés à l'échelle nationale et à l'étranger) des organismes sans but lucratif, comme CyberNB. Plus du tiers des personnes interrogées ont également parlé du soutien des programmes d'éducation de la petite enfance par la province, comme CyberTitan[15], qui inspirent et attirent les jeunes dans le domaine. Pour soutenir encore davantage la place centrale accordée au volet pédagogique par la province, 80 % des répondants ont mentionné leur engagement à l'égard des établissements d'enseignement de la maternelle à la 12e année et de niveau postsecondaire, défendant les enjeux associés au perfectionnement de la main-d'œuvre et les occasions de reconnaissance par l'industrie de façon indépendante pour les jeunes, 60 % le faisant en dehors de leurs obligations professionnelles. Le lien étroit entre l'industrie de la cybersécurité et les efforts de formation et de perfectionnement de la main d'œuvre renferment un contexte fondamental pour comprendre l'offre et la demande en cybersécurité dans la province du Nouveau-Brunswick.

[15] *CyberTitan, "Canadian Youth Cyber Education Initiative," 2020. https://www.cybertitan.ca/*

COMPRENDRE LA DEMANDE EN CYBERSÉCURITÉ

Canada et au Nouveau-Brunswick

Les entreprises, les gouvernements, les associations d'industries et les autres organisations du Canada, du Nouveau-Brunswick et du reste du monde connaissent un besoin accru pour des employés ayant de l'expérience en cybersécurité. Le personnel en cybersécurité occupe des rôles notamment de « pirates éthiques », lesquels testent les limites des stratégies de sécurité existantes, de stratèges de haut niveau en cybersécurité, ou encore de spécialistes des bases de données ou du matériel informatique. Une étude réalisée en 2017 auprès de quelque 20 000 professionnels de la cybersécurité de 170 pays prédisait une pénurie mondiale de main-d'œuvre en cybersécurité de 1,8 million de personnes d'ici 2022, et une pénurie nord-américaine équivalente de 265 000 personnes d'ici cette même année[16]. Le présent document cherche à comprendre la demande de personnel en cybersécurité au Nouveau Brunswick, à déterminer si la province fera face ou non à un manque de main-d'œuvre dans le domaine, et à définir les tendances de l'emploi en cybersécurité et des besoins en compétences.

La demande en cybersécurité : Ampleur et tendances au fil du temps

À tous les égards, la demande en cybersécurité est grande autant au Canada qu'au Nouveau-Brunswick. Différentes approches pour évaluer la demande en cybersécurité révèlent cependant des tendances distinctes. Bien qu'une évaluation de l'emploi par Statistique Canada souligne de faibles taux de chômage au sein des rôles associés à la cybersécurité et puisse illustrer des tendances au fil du temps, des outils plus précis, comme le sondage auprès des employeurs en cybersécurité du Nouveau Brunswick[17] réalisé par le CTIC, une analyse détaillée des avis d'emploi en cybersécurité et les perspectives des intervenants clés de l'industrie, dressent un portrait plus granulaire des forces en jeu dans l'embauche de talents en cybersécurité dans la province.

Mesure de l'emploi au moyen de la Classification nationale des professions

Présentement, aucune Classification nationale des professions (CNP)[18] unique ne représente tous les rôles en cybersécurité. Cependant, le CTIC a ciblé des codes professionnels associés à la cybersécurité dans les données nationales afin de pouvoir établir des tendances de l'emploi dans ce domaine dans l'ensemble du Canada et par province[19]. Ils sont les suivants :

0213 Gestionnaires des systèmes informatiques

2171 Analystes et consultants en informatique

2172 Analystes de bases de données et administrateurs de données

2281 Techniciens de réseau informatique

2283 Évaluateurs de systèmes informatiques

[16]Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, 2017, p. 2.
[17]Le sondage réalisé par le CTIC auprès des employeurs a été distribué à l'automne 2019. Ce sondage ciblait toute entreprise du Nouveau Brunswick employant du personnel dans le secteur de la cybersécurité, et sa portée touchait des sociétés d'experts-conseils en cybersécurité, de grandes entreprises technologiques et d'autres secteurs connexes. Pour de plus amples renseignements sur le sondage réalisé par le CTIC auprès des employeurs, consultez l'annexe I.
[18]Il s'agit de la mesure normalisée de la main-d'œuvre utilisée par Statistique Canada dans le cadre d'instruments comme l'Enquête sur la population active et le recensement.
[19]Conseil des technologies de l'information et des communications (CTIC). « Forecasting Demand for Cybersecurity Workers in Canada: 2017-2023 » : https://www.ictc-ctic.ca/wp-content/uploads/2019/02/ICTC_Forecast-Cybersecurity_1.31.19.pdf

Le gouvernement du Nouveau-Brunswick estimait que 4 732 personnes travaillaient en cybersécurité dans la province en 2018, ou 0,6 % de la population totale de la province pour l'année visée[20].

Des rapports internationaux sur le manque de main-d'œuvre en cybersécurité vantent des taux de chômage mondiaux aussi bas que 0 %[21]. Pour comprendre les tendances en matière de cybersécurité au fil du temps, il est important d'établir un portrait du chômage propre à la province.

Dans l'ensemble, bien que le taux de chômage dans le domaine de la cybersécurité au Nouveau Brunswick ne soit pas nul, il est clair que l'emploi dans le sous-secteur de la cybersécurité surpasse le secteur général de la technologie (TIC) et l'emploi en général. La **figure 1** souligne les différences entre le taux de chômage en cybersécurité au Nouveau-Brunswick, le taux de chômage en TIC dans la province, ainsi que les taux moyens de chômage à l'échelle provinciale et nationale. Malgré une tendance légèrement à la hausse du taux de chômage au cours des cinq dernières années, les travailleurs en cybersécurité au Nouveau-Brunswick sont beaucoup moins susceptibles d'être au chômage que le reste de la main-d'œuvre de la province, tout comme les travailleurs du secteur des TIC. Aussi, le taux de chômage chez les travailleurs en TIC et cybersécurité de la province est beaucoup moins élevé que la moyenne canadienne (dans l'ensemble des industries) : en 2019, le Nouveau Brunswick enregistrait un taux de chômage de 1,24 % pour les travailleurs en cybersécurité et de 2,94 % pour les travailleurs en TIC, tandis que la moyenne canadienne était de 5,66 % et que l'équivalent provincial au Nouveau-Brunswick était de 7,95 %.

Taux de chômage au fil du temps

Nouveau-Brunswick : Secteur des TIC et cybersécurité, et ensemble du Canada

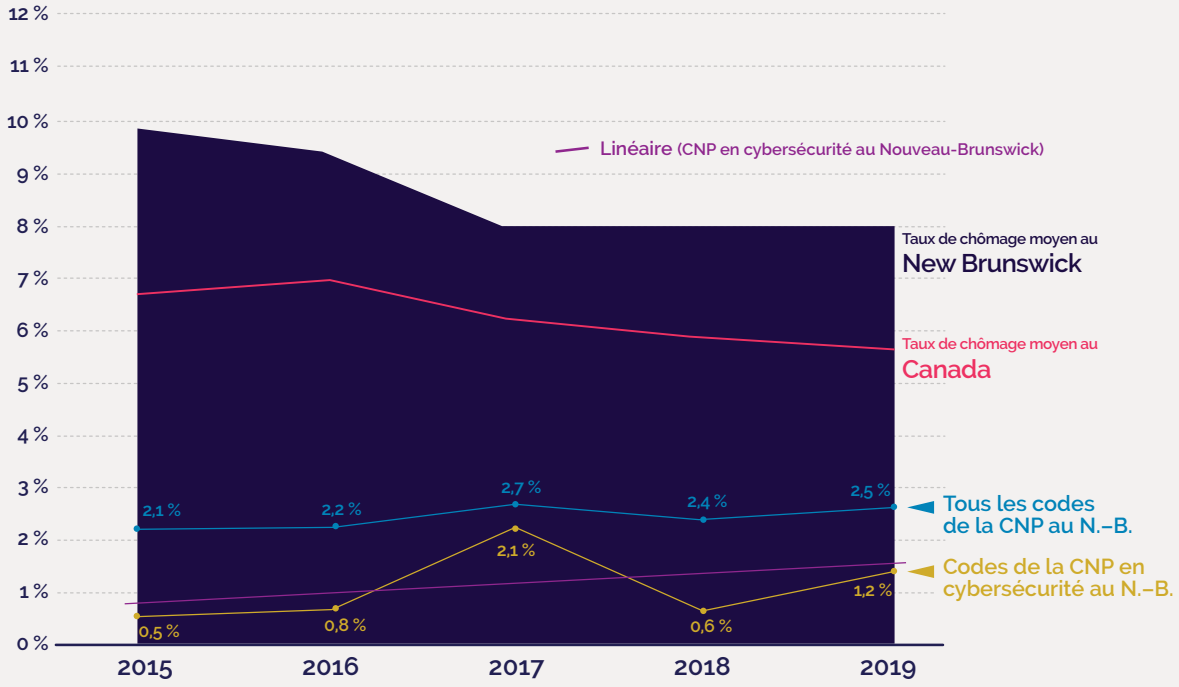


Figure 1 : Taux de chômage au fil du temps : Groupes des CNP en TIC et cybersécurité au Nouveau-Brunswick comparés aux taux de chômage moyens au Canada et au Nouveau-Brunswick, 2015-2019, Enquête sur la population active de Statistique Canada. Les données supprimées par Statistique Canada sont exclues de ce tableau dans la détermination des moyennes annuelles. Voir l'annexe I pour d'autres détails.

[20]Gouvernement du Nouveau-Brunswick. www.emploisnb.ca. Consulter l'annexe I pour voir les emplois associés à ces CNP en 2018.
[21]Voir, par exemple, des histoires comme celles de Mack Gelber, « This tech filed just hit an astonishing 0% unemployment rate », Monster, sans date : https://www.monster.com/career-advice/article/tech-cybersecurity-zero-percent-unemployment-1016.

La légère tendance à la hausse du taux de chômage dans le secteur de la cybersécurité au cours des cinq dernières années est un schéma intéressant. Surtout, cette tendance peut ou peut ne pas être liée aux emplois de chaque code de la CNP qui se rapporte à la cybersécurité précisément puisque chacun des cinq CNP comprend plusieurs titres d'emploi, certains étant directement liés à la sécurité et d'autres non (par exemple, un gestionnaire de TI peut être responsable ou non de la sécurité numérique de son organisation). Afin de comprendre la demande pour des emplois en cybersécurité, la prochaine section, intitulée Le marché de la cybersécurité du Nouveau-Brunswick : Les compétences et les emplois recherchés, examine encore davantage les rôles en cybersécurité à l'aide de données probantes autres que celles disponibles auprès de Statistique Canada. Néanmoins, comme l'illustre la **figure 2** ci-dessous, les 5 professions liées à la cybersécurité ont connu un taux de croissance annuel composé de 3,0 % au cours des 15 dernières années dans la province. Par conséquent, si le taux de chômage et le nombre d'emplois en cybersécurité augmentent (quoique seulement très légèrement dans le cas du taux de chômage), il est possible que l'approvisionnement en main-d'œuvre pour l'un ou l'autre de ces codes de la CNP dépasse la demande, globalement. Comme le présent document l'examinera dans les prochaines sections, les types d'emplois recherchés en cybersécurité, qui tendent à être des rôles qui exigent une plus grande expérience professionnelle que ce que peut offrir un récent diplômé, pourraient expliquer partiellement la situation. À ce titre, et comme le démontrera la section intitulée Le marché de la cybersécurité du Nouveau-Brunswick : Les compétences et les emplois recherchés, alors que de nombreux rôles en cybersécurité sont très recherchés, ils sont aussi les plus difficiles à doter sans un degré élevé de spécialisation. De plus, ces tendances pourraient encore une fois s'expliquer par le nombre d'emplois au sein de chaque code de la CNP qui ne s'applique pas directement à la cybersécurité.

Emplois en cybersécurité au fil du temps

Nouveau-Brunswick

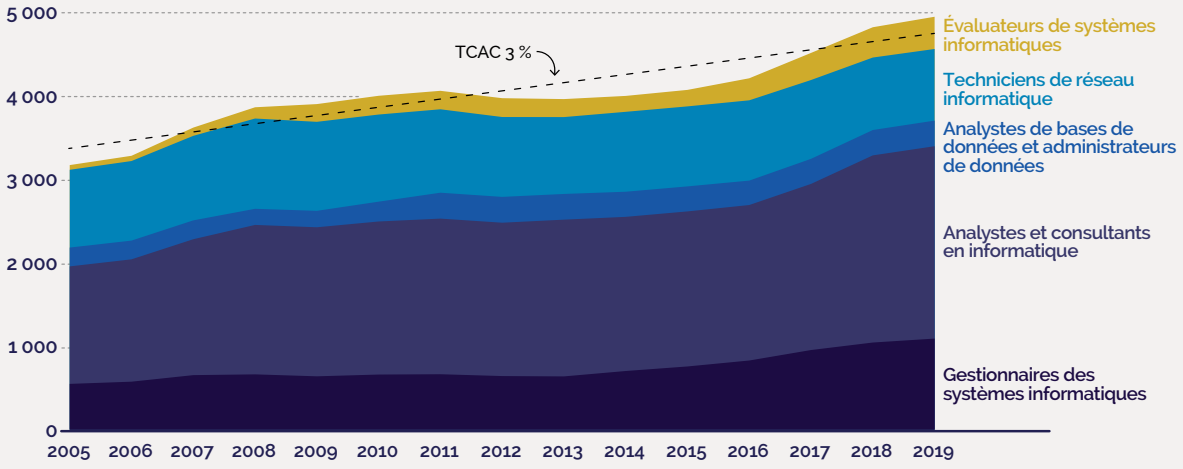
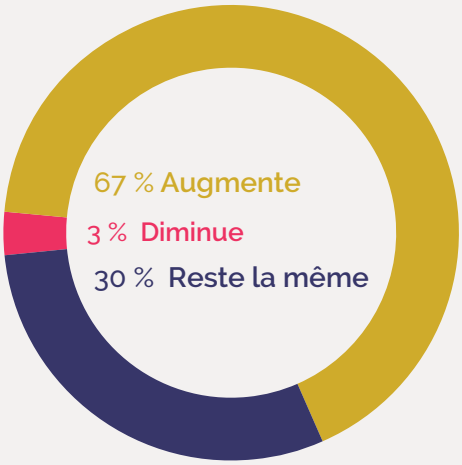


Figure 2 : Nombre d'emplois dans chacun des 5 codes de la CNP liés à la cybersécurité dans la province du Nouveau Brunswick, de 2005 à 2019, représentant 15 années de croissance de l'emploi et un taux de croissance annuel composé de 3,0 %. Source : Statistique Canada

D'autres données probantes, ciblant davantage la cybersécurité que les codes de la CNP, soulignent aussi un nombre croissant d'emplois pour les travailleurs qui œuvrent à combattre et à prévenir la cybercriminalité au Nouveau-Brunswick. Dans le cadre du sondage mené par le CTIC auprès d'employeurs en 2019, les deux tiers des répondants (67 %) estimaient que leur main-d'œuvre en cybersécurité augmenterait au cours de la prochaine année, et de ce nombre, plus de la moitié (60 %) croyaient qu'elle augmenterait de 2 employés ou plus (voir la **figure 3**).

Au cours de la prochaine année, vous vous attendez à ce que votre main-d'œuvre en cybersécurité au Nouveau-Brunswick...



Combien d'employés en cybersécurité aimeriez-vous idéalement embaucher au Nouveau-Brunswick au cours de la prochaine année?

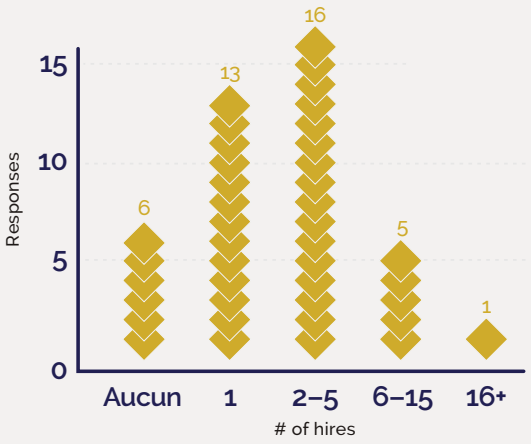


Figure 3 : Évaluations des employeurs en cybersécurité quant au nombre d'employés qu'ils comptent embaucher au cours de la prochaine année. Les attentes raisonnables des employeurs sont présentées à gauche, alors que les scénarios idéaux des employeurs sont énoncés à droite. Source : CTIC

Alors que bon nombre d'employeurs promettent d'accroître leur main-d'œuvre au cours de la prochaine année, le fait que seulement 3 % des employeurs anticipent une baisse de leur main-d'œuvre dans la figure de gauche (évaluant les attentes d'une hausse ou d'une baisse réaliste) est encore plus étonnant.

Les promesses des employeurs de développer leur main-d'œuvre sont appuyées par une analyse des avis d'emplois dans la province. Au cours des six derniers mois, le CTIC a recueilli des informations sur les sites d'emplois au Nouveau-Brunswick au sujet de la fréquence et des types d'emplois en cybersécurité annoncés. Bien qu'une analyse détaillée des avis d'emplois par type de rôle soit présentée ultérieurement dans le présent rapport, la **figure 4** illustre quelques faits saillants concernant les avis d'emplois en cybersécurité dans la province. Le nombre de nouveaux avis par mois suggère un retard dans l'embauche avant la période des Fêtes, mais il y a en moyenne 7,5 nouveaux rôles affichés par mois pour la période au cours de laquelle le CTIC a recueilli des données. En ce qui concerne les avis d'emplois en cybersécurité par ville, Fredericton et Saint John sont des chefs de file reconnus dans la province, bénéficiant en plus de la présence d'employeurs majeurs dans leurs régions : IBM est un chef de file en matière d'embauche à Fredericton, Irving Oil fait de même à Saint John, et Mariner en est un à Saint John et à Moncton.

Avis d'emplois en cybersécurité au Nouveau-Brunswick

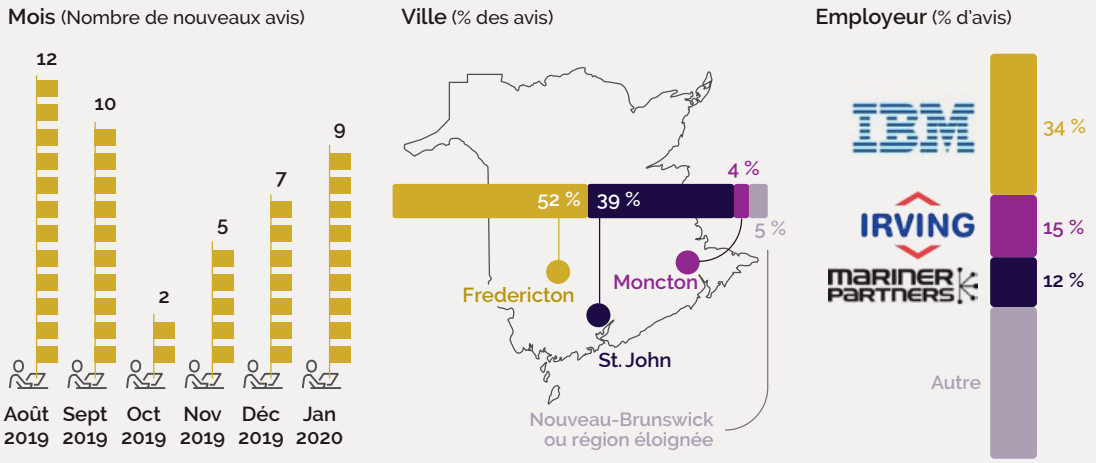


Figure 4 : Source, CTIC

Le CTIC a également recueilli des informations sur les sites d'emplois en cybersécurité dans le reste du Canada. La **figure 5** montre une tendance que le Nouveau-Brunswick partage avec d'autres provinces canadiennes : dans l'ensemble, une baisse du nombre d'avis d'emplois en cybersécurité peut être observée à l'automne, surtout en octobre, alors qu'une hausse est observée au début de la nouvelle année. Le nombre d'avis par mois au Nouveau-Brunswick correspond étroitement à la moyenne canadienne (tirée de l'éventail d'avis affichés dans toutes les provinces).

Pourcentage des avis d'emplois en cybersécurité par mois

Août 2019 à janvier 2020

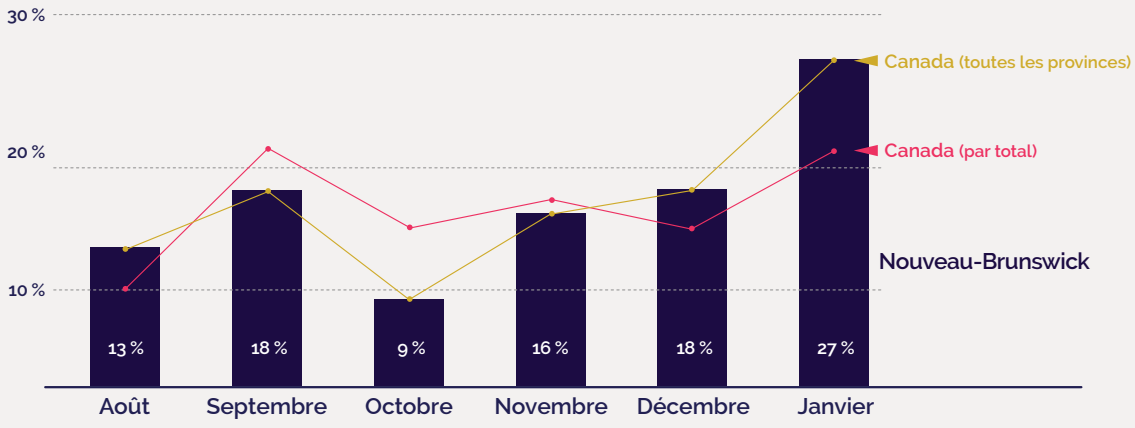


Figure 5 : Comparaison entre le nombre brut d'avis affichés (nouveaux et anciens) par mois : Nouveau-Brunswick, Canada, selon le total des avis affichés, Canada par médiane (toutes les provinces). Source : CTIC, 2020.

Ces données sur les avis d'emplois peuvent aussi être examinées en comparant la part de la population canadienne de chaque province au nombre d'avis d'emplois en cybersécurité, constatant que l'Ontario, la Nouvelle-Écosse, l'Île-du-Prince-Édouard et le Nouveau-Brunswick enregistrent des résultats de niveau égal ou supérieur à ce que leur population suggère qu'elles le devraient.

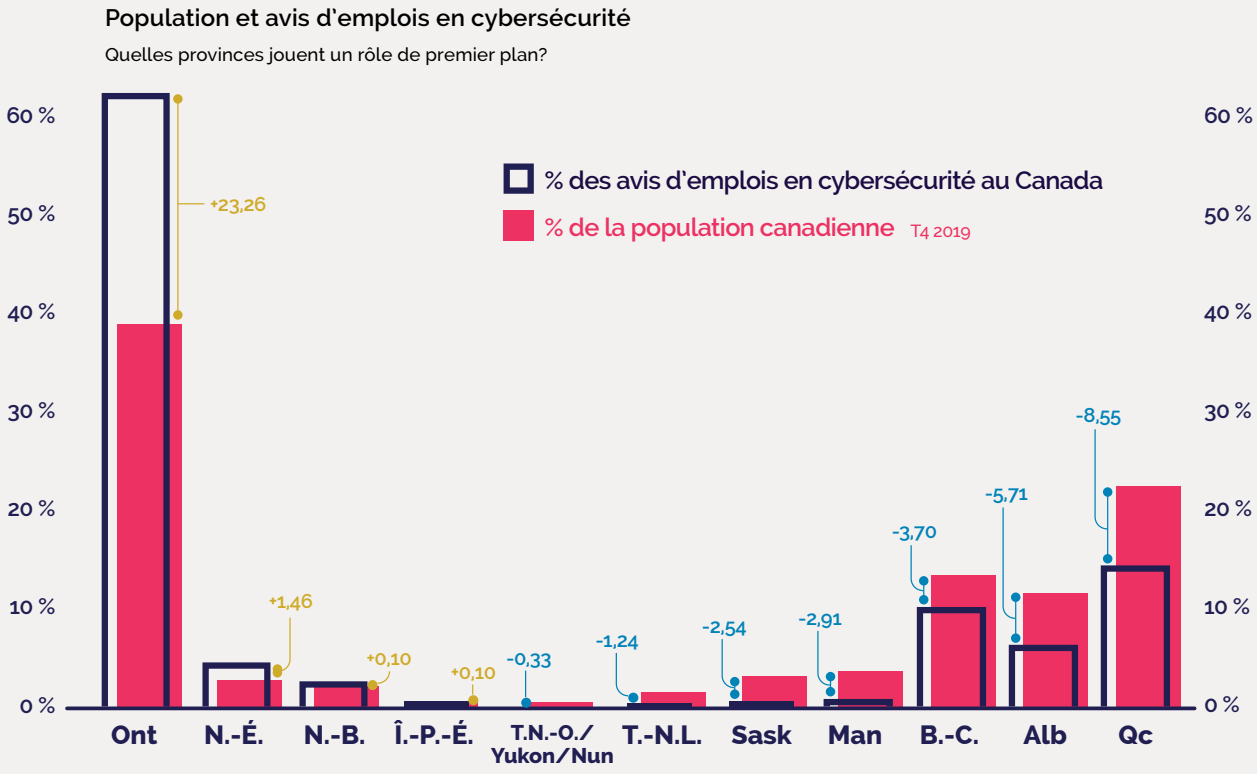


Figure 6 : Part de la population canadienne des provinces et des territoires comparée au nombre de rôles affichés en cybersécurité. Les données sur les avis d'emplois datent de janvier 2020. Source : CTIC, Statistique Canada.

La demande en cybersécurité : Employeurs par secteur et taille

Les professionnels de la cybersécurité travaillent notamment pour des entreprises et des organisations spécialisées en cybersécurité, des établissements d'enseignement ou des organismes gouvernementaux, ou encore comme spécialistes dans une grande variété de secteurs. Cependant, bon nombre de travailleurs dans le domaine sont des généralistes des TI à qui une responsabilité de cybersécurité a été confiée. Il n'est donc pas surprenant de constater que les grandes organisations du Canada investissent plus fréquemment pour embaucher du personnel de cybersécurité , et c'est également vrai pour les répondants au sondage du CTIC au Nouveau-Brunswick : tandis que près du tiers (29,6 %) des petites entreprises (moins de 100 employés) ont indiqué ne disposer d'aucun professionnel de la cybersécurité,[23] seulement 1 des 14 entreprises de grande et moyenne taille (plus de 100 employés) ont signalé la même chose[24].

Dans l'ensemble du Canada et au Nouveau-Brunswick, de nombreuses industries emploient des professionnels de la cybersécurité. La **figure 7** montre les industries les plus susceptibles d'employer au moins quelques professionnels de la cybersécurité, en commençant par les finances et l'assurance, où 91,6 % du secteur au Canada emploie au moins un professionnel responsable de la cybersécurité. Notamment, dans le contexte canadien, les secteurs des services publics et des ressources naturelles (p. ex. production pétrolière et gazière et énergie nucléaire) sont des ajouts importants à la liste d'employeurs potentiels en cybersécurité, une tendance d'une grande pertinence dans le contexte du Nouveau-Brunswick.

Force de la main-d'œuvre en cybersécurité dans les 10 principales industries employant du personnel en cybersécurité au Canada

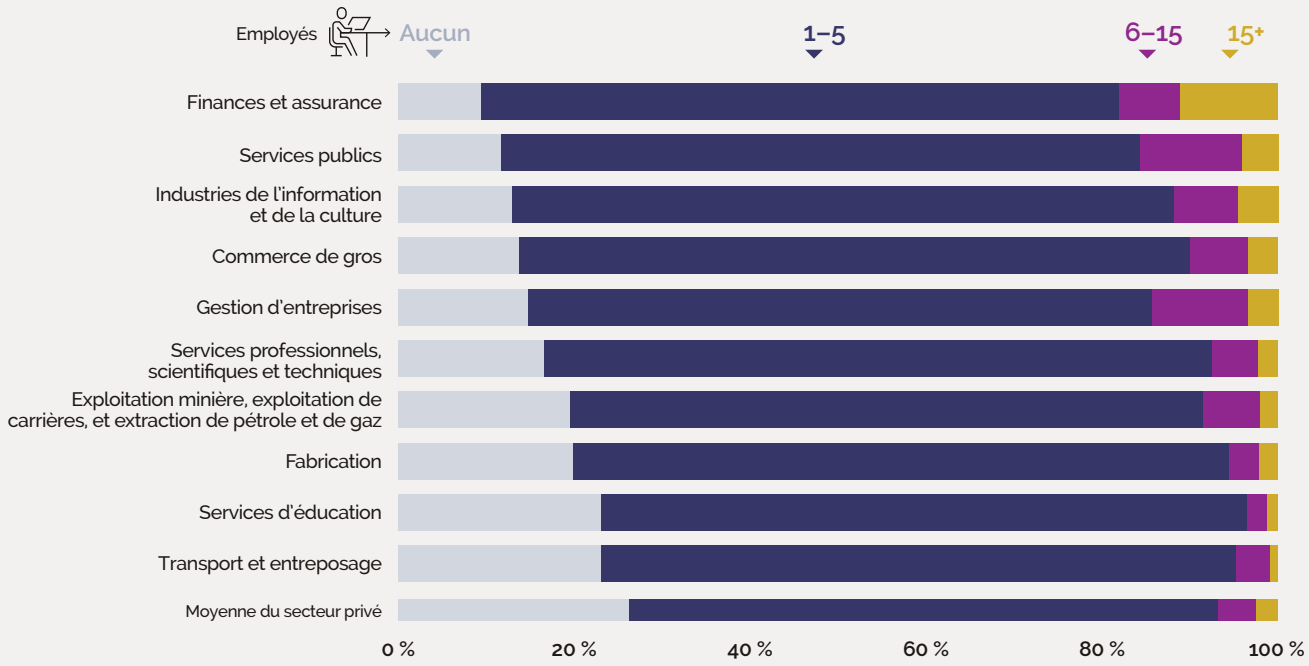


Figure 7 : Pourcentage des entreprises indiquant le nombre d'employés principalement responsables de la cybersécurité en général, y compris les 10 principales industries qui sont les plus susceptibles d'employer au moins un responsable de la cybersécurité, ainsi que la moyenne dans le secteur privé. Source : Enquête canadienne sur la cybersécurité et le cybercrime de 2017 de Statistique Canada

[23]Ces nouveaux professionnels de la cybersécurité travaillent au sein d'entreprises de différentes tailles, mais surtout pour les grandes entreprises. Le sondage sur l'adoption des TIC réalisé par la Chambre de commerce du Canada en 2017 a révélé que la taille d'une entreprise jouait un rôle important dans l'ampleur de ses investissements en cybersécurité : alors que 85 % des grandes entreprises interrogées ont formé du personnel en cybersécurité dans une période 3 mois, seulement 26 % des microentreprises et 45 % des petites entreprises ont fait de même.
[24]Source : Sondage auprès des employeurs en cybersécurité au Nouveau-Brunswick, CTIC, 2019.

Toutefois, les industries ne se pressent pas toutes pour embaucher du personnel en cybersécurité. Dans le même sondage pancanadien, les entreprises qui n'avaient pas embauché de professionnels de la cybersécurité ont précisé deux principales raisons pour cette disparité : (a) ils avaient recours à des consultants externes plutôt qu'à leur propre personnel, ou (b) ils estimaient que la cybersécurité de leur entreprise n'était pas suffisamment menacée. L'expertise-conseil en cybersécurité inclut une grande partie du secteur de la cybersécurité, et bon nombre d'organisations ont recours à des consultants lorsqu'elles n'ont pas les ressources nécessaires ou n'ont pas besoin d'embaucher des employés précisément à cette fin. Les deux principales raisons pour lesquelles les répondants n'embauchent pas de personnel de cybersécurité sont présentées par industrie à la **figure 8**.

Deux principales raisons de ne pas employer de professionnels responsables de la cybersécurité

par industrie, Canada, 2017

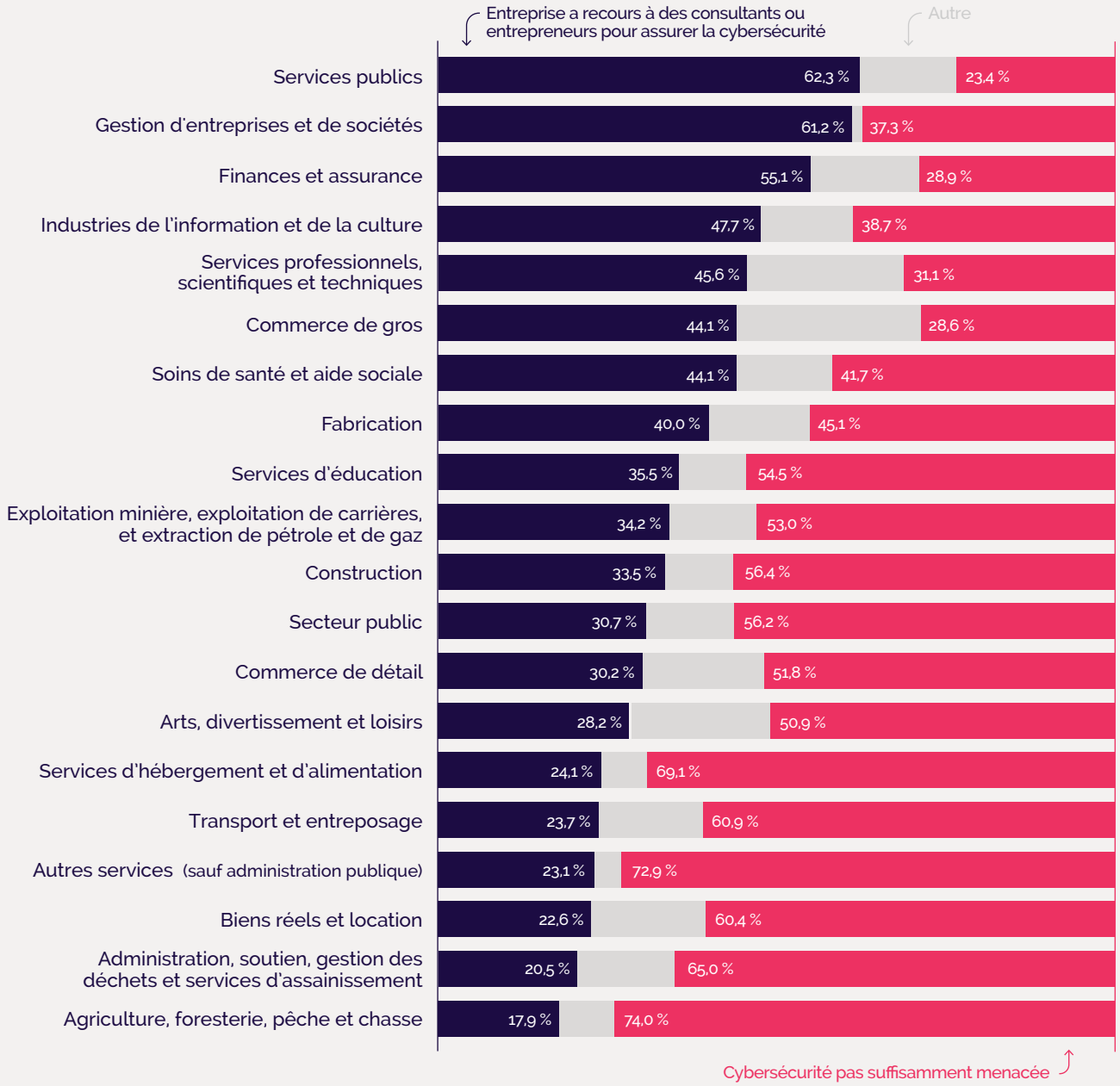


Figure 8 : Des répondants qui ne disposent pas de personnel dédié à la cybersécurité, % estime que
Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime, 2017.

Dans l'ensemble du secteur privé en 2017, 74 % des entreprises canadiennes employaient des responsables de la cybersécurité, une situation plus fréquente dans les entreprises de grande et moyenne taille[25]. De même, au Nouveau-Brunswick, 75 % des répondants au sondage auprès des employeurs employaient au moins un responsable de la cybersécurité, et la majorité des organisations sans personnel de cybersécurité (80 %) employaient moins de 100 personnes globalement[26]. En d'autres termes, les plus petites entreprises, autant au Nouveau-Brunswick qu'au Canada, sont moins susceptibles d'employer un personnel dédié à la cybersécurité.

Parmi les entreprises canadiennes qui ne disposaient pas de personnel de cybersécurité (26 %), environ la moitié ont indiqué qu'elles n'étaient pas suffisamment exposées à des risques en la matière (bien qu'aucune entreprise du Nouveau-Brunswick n'ait formulé le même commentaire : voir **figure 9**)[27], alors qu'environ le tiers d'entre elles avaient recours à des consultants ou à des entrepreneurs plutôt que d'employer du personnel sur place (31 %)[28]. La figure 9 compare les raisons pour lesquelles les répondants au sondage au Nouveau-Brunswick n'embauchent pas de personnel de cybersécurité aux moyennes du secteur des TIC et du secteur privé du Canada. Dans l'ensemble, les répondants au sondage au Nouveau-Brunswick ont précisé qu'ils reconnaissaient les risques pour la cybersécurité, qu'ils étaient plus susceptibles de faire appel à des entrepreneurs en cybersécurité, et qu'ils avaient recours à une assurance de cyber-responsabilité, des réponses fréquentes, mais probablement attribuables au type de répondants enclins à répondre à un sondage sur le thème de la cybersécurité. Alors qu'un plus grand nombre d'entreprises du Nouveau-Brunswick ont indiqué ne pas disposer des ressources adéquates pour employer un professionnel de la cybersécurité, les entreprises néo-brunswickoises et canadiennes estimaient qu'elles étaient tout simplement incapables de trouver des professionnels qualifiés.

Les principales raisons pour lesquelles elles n'emploient pas de personnel principalement responsable de la cybersécurité

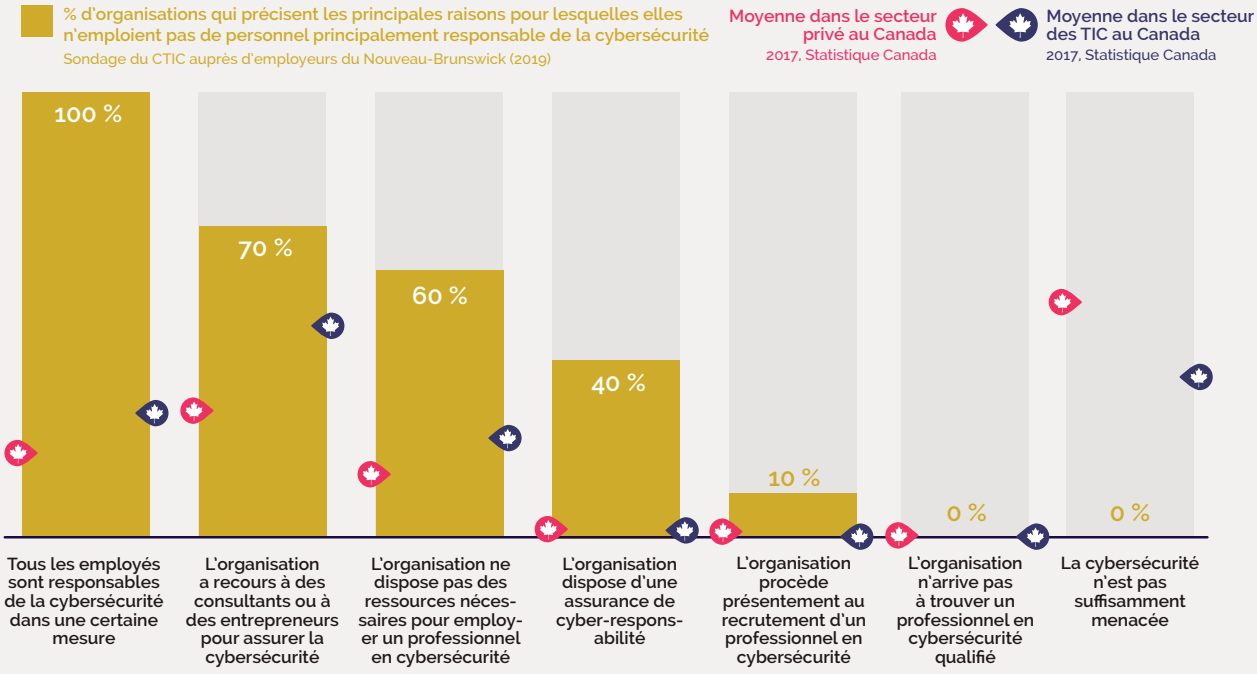


Figure 9 : Comparaison des raisons des entreprises du Canada et du Nouveau-Brunswick de ne pas employer du personnel principalement responsable de la cybersécurité. Comparaison tirée de deux instruments de recherche différents (sondage du CTIC mené en 2019 auprès des employeurs et Enquête canadienne sur la cybersécurité et le cybercrime de 2017 de Statistique Canada). Alors que la formulation et la structure des questions des sondages étaient identiques, les types de réponses peuvent différer en raison de l'ordre des questions et des différences entre les répondants ciblés

[25]Statistique Canada, L'incidence du cybercrime sur les entreprises canadiennes, 2017.
[26]Sondage auprès des employeurs en cybersécurité au Nouveau-Brunswick, CTIC, 2019.
[27]Cependant, cette comparaison est tirée de deux sources de données très différentes. Alors que le sondage auprès des employeurs en cybersécurité au Nouveau-Brunswick du CTIC et l'Enquête canadienne sur la cybersécurité et le cybercrime de Statistique Canada ont utilisé les mêmes options de réponses, le sondage du CTIC ciblait des organisations connues pour employer du personnel de cybersécurité, alors que Statistique Canada a échantillonné l'ensemble du secteur privé.
[28]Statistique Canada, L'incidence du cybercrime sur les entreprises canadiennes, 2017.

LE MARCHÉ DE LA CYBERSÉCURITÉ DU NOUVEAU BRUNSWICK :

Les compétences et les emplois recherchés

Comprendre la composition de la main-d'œuvre et la demande au moyen du cadre NICE

Les professionnels de la cybersécurité sont des investissements de plus en plus essentiels pour les entreprises canadiennes : dans l'ensemble, les entreprises du Canada ont dépensé 8 milliards de dollars pour les salaires des employés, des consultants et des entrepreneurs en 2017[29]. Les catégories fournies par le cadre NICE[30] sont une bonne façon de comprendre la décomposition des rôles du personnel de cybersécurité. Ce cadre américain a été adopté par des organisations du monde entier dans le but d'opter pour une terminologie normalisée des emplois et des compétences en cybersécurité, et il décompose la main-d'œuvre en sept principaux types de rôles qui permettront de comprendre la composition de la main-d'œuvre et la demande dans l'analyse à venir[31].

> *Nous voulons que la cybersécurité soit une seule langue dans le monde entier. Si vous suivez un cours en Australie, il correspondra à la formation offerte au Canada et aux États-Unis. Lorsque les emplois sont affichés, tout correspond. Le cadre favorise vraiment un lexique commun.*
>
> - Dillon Donahue, CyberNB

Une autre des personnes interrogées laissait entendre que l'adoption du cadre NICE dans la province était en grande partie attribuable au leadership des partenaires académiques. En prenant le temps de mieux comprendre et d'évaluer la valeur d'un cadre cohérent dans l'industrie, le milieu universitaire a commencé à modifier les résultats des programmes afin de s'harmoniser plus étroitement avec les critères de compétences et les dénominations du cadre NICE.

[29]Statistique Canada, L'incidence du cybercrime sur les entreprises canadiennes, 2017.
[30]Ce cadre a été élaboré initialement par le département du Commerce des États-Unis comme effort collaboratif entre l'industrie et le milieu universitaire afin de mieux définir, évaluer et comprendre la diversité de la main-d'œuvre en cybersécurité. Newhouse, W., Keith, S., Scribner, B., et Witte, G. Cadre sur la main-d'œuvre en cybersécurité de la National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology, 2017 : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf, p. 11.
[31]Cadre sur la main-d'œuvre en cybersécurité de la National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology, 2017 : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf. Au moment de la rédaction, CyberNB a indiqué son intention de créer un version du cadre NICE propre au Nouveau-Brunswick. Emploi et Développement social Canada a demandé à l'Association canadienne de la technologie de l'information de créer une version canadienne.

	Catégories	Descriptions[32]	Titres d'emplois fréquents au Canada[33]
SA	Sécuriser l'approvisionnement	Conceptualise, conçoit, fournit ou établit des systèmes sécuritaires de technologies de l'information, et assume des responsabilités liées aux aspects des systèmes ou du développement de réseaux.	• Gestionnaire de la sécurité et des risques • Architecte des systèmes et de la sécurité • Développeur et planificateur de logiciels et de systèmes • Analyste de la sécurité
OM	Opérer et maintenir	Veille au soutien, à l'administration et à la maintenance nécessaires pour assurer la sécurité et le rendement efficaces des systèmes de technologies de l'information.	• Administrateur de la sécurité ou des données et des bases de données • Gestionnaire du savoir ou des risques pour la sécurité • Représentant du soutien technique ou d'assistance à la clientèle • Administrateur et analyste des réseaux et des systèmes
ER	Encadrer et régir	Assure le leadership, la gestion, l'orientation, le développement et la promotion afin que l'organisation fasse son travail de cybersécurité efficacement.	• Responsable principal de la sécurité de l'information • Analyste des stratégies de cybersécurité • Analyste des politiques de cybersécurité • Analyste des cybercommunications • Gestionnaire des programmes de cybersécurité • Gestionnaire de projets et des acquisitions
PD	Protéger et défendre	Recense, analyse et atténue les menaces contre les réseaux ou les systèmes internes de technologies de l'information.	• Analyste de la cybersécurité • Ingénieur en infrastructures de sécurité et cyberdéfense • Intervenant en incidents de cybersécurité • Analyste des vulnérabilités • Gestionnaire de centre d'opérations de sécurité
AN	Analyser	Effectue un examen et une évaluation hautement spécialisés des informations entrantes de cybersécurité pour déterminer leur utilité en matière de renseignement	• Analyste des renseignements sur les menaces • Gestionnaire de l'analyse en cybersécurité • Scientifique des données • Analyste langagier et linguiste informaticien
RO	Recueillir et opérer	Effectue des opérations spécialisées de déni et de déception, et recueille des informations de cybersécurité qui pourraient être utilisées pour développer des renseignements	• Pirate éthique et opérateur en cybercollection • Planificateur de la sécurité cyberopérationnelle • Chasseur de menaces et cyberopérateur
EN	Enquêter	Réalise des enquêtes sur les incidents de menace à la cybersécurité ou les crimes liés aux systèmes de technologies de l'information, aux réseaux et aux preuves numériques	• Analyste en cybersécurité et criminalistique numérique • Enquêteur en cybersécurité

Figure 10 : Catégories de main-d'œuvre du cadre NICE

[32]Cadre sur la main-d'œuvre en cybersécurité de la National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology, 2017 : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
[33]Selon l'information fournie par CyberNB, ainsi qu'une publication de 2018 de Deloitte reliant le cadre NICE au contexte canadien : Deloitte et Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018.

Un petit nombre de partenaires de l'industrie ont exprimé des préoccupations quant à l'origine américaine du cadre (et donc son applicabilité au contexte canadien), particulièrement en ce qui concerne la tendance du marché canadien à annoncer des rôles généraux qui s'inscrivent dans plusieurs catégories du cadre NICE. Advenant l'adoption élargie du cadre, les chefs de file de l'industrie des petites et moyennes entreprises estiment qu'il pourrait entraîner des descriptions de travail trop précises et restrictives, ce qui limiterait l'embauche de talents internationaux ou de personnes n'ayant pas de compétences techniques ou universitaires. Toutefois, les personnes interrogées ont également indiqué que ce problème pourrait être réglé s'il existait un consensus international plus large quant à l'utilisation du cadre.

> *Nous devons tous travailler ensemble et comprendre que ce n'est pas seulement le Nouveau-Brunswick, l'Ontario ou même le reste du Canada qui doit adopter le cadre NICE. Nous ne voulons simplement pas qu'un candidat hautement qualifié de l'Europe ou du Moyen-Orient se retrouve à occuper un rôle pour lequel il est surqualifié simplement parce nous ne comprenons pas son éducation.*
>
> - Dillon Donahue, CyberNB

Les avantages d'utiliser un cadre qui est de plus en plus cohérent à l'échelle internationale semblent éclipser les préoccupations partagées par les représentants de l'industrie à plus grande échelle. Bon nombre de répondants ont déjà commencé à redévelopper les résultats de leurs programmes et leurs processus d'embauche afin de mieux refléter la norme de l'industrie. De plus, les organisations ayant des liens étroits avec les marchés américains ou internationaux (par le biais d'autres lieux, clients ou partenaires) ont indiqué que l'adoption de ce cadre clarifiait et facilitait les processus d'immigration et l'obtention de visas.

Taux de croissance des professions en cybersécurité

Alors que le taux de chômage est faible chez les professionnels de la cybersécurité au Nouveau Brunswick (comme le montre la **figure 1** ci-dessus), certaines professions sont clairement plus recherchées que d'autres. La **figure 11** ci-dessous présente chaque code de la CNP en comparant deux valeurs différentes : le nombre brut d'emplois d'un code précis au Nouveau-Brunswick en 2019 et le taux de croissance moyen annuel sur 5 ans (TCAM, 2015-2019) qui montre dans quelle mesure cet emploi prend de l'ampleur au fil du temps. Par exemple, alors que les évaluateurs de systèmes informatiques ne représentent que 386 emplois, ils ont connu une très forte croissance en moyenne (15,7 %) au cours des 5 dernières années. En tenant compte du nombre brut d'emplois et du taux de croissance, il est clair que trois catégories d'emplois continuent d'obtenir de bons résultats (quant au nombre de personnes employées et à la croissance à venir) au Nouveau-Brunswick. Par comparaison, deux professions enregistrent un rendement inférieur. Les analystes de bases de données et les administrateurs de données enregistrent de faibles nombres et une croissance limitée. Les chiffres concernant les administrateurs de réseaux informatiques sont relativement élevés, mais la croissance est négative d'une année sur l'autre, suggérant que le nombre d'emplois au sein de ces professions restera bas ou diminuera lentement au fil du temps.

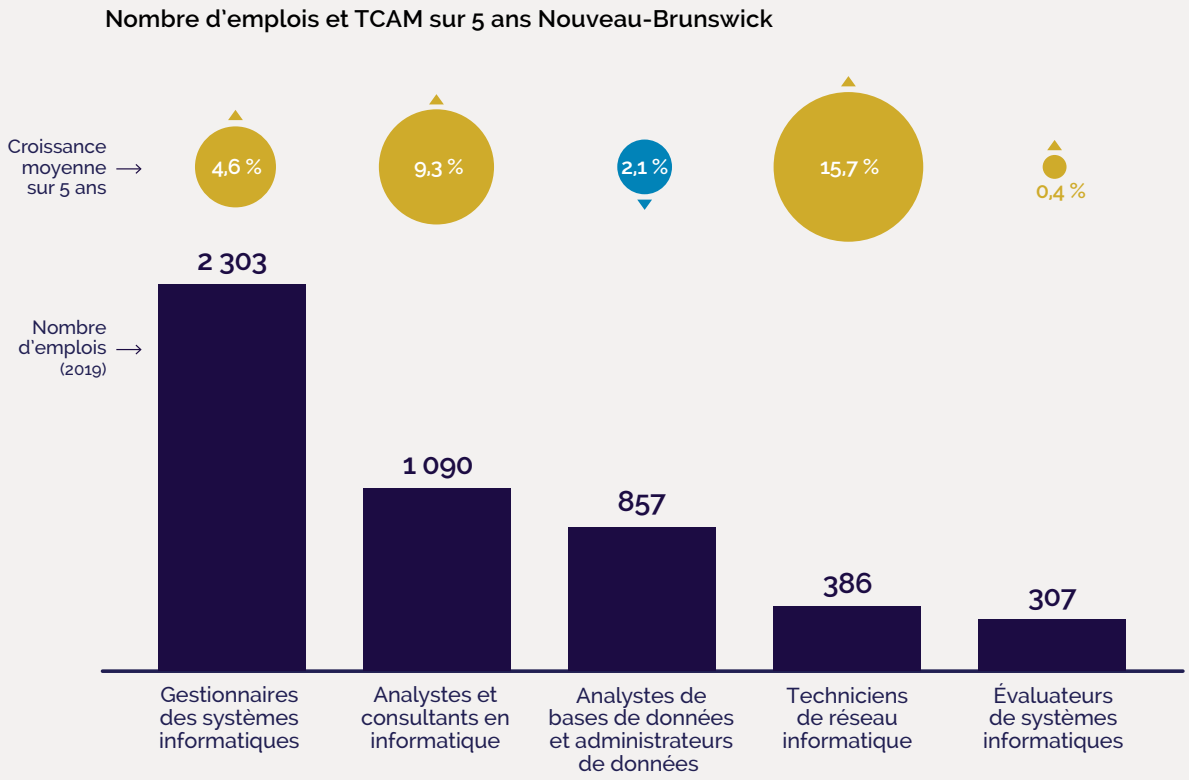


Figure 11 : Comparaison du nombre brut d'emplois en 2019 pour chacune des cinq professions en cybersécurité et du TCAM sur cinq ans pour chaque rôle. Source : Statistique Canada.

Afin de comparer les conclusions de Statistique Canada à d'autres sources de données, chaque catégorie de la CNP peut être globalement liée au cadre NICE. Il est important de noter que cette comparaison n'est qu'illustrative, et non concluante, puisqu'il ne s'agit pas d'une concordance un pour un : les codes de la CNP et le cadre NICE ne sont pas directement liés, et les nombreux titres d'emploi qui tombent sous chaque catégorie de la CNP pourraient être attribués à une variété de catégories du cadre. À ce titre, la **figure 12** ci-dessous représente le modèle qui convient le mieux. Lorsque les cinq catégories de la CNP en cybersécurité sont jumelées aux catégories du cadre NICE comme à la figure 10, il est évident que les trois catégories enregistrant le meilleur rendement s'harmonisent mieux avec deux catégories du cadre NICE : sécuriser l'approvisionnement (1) et encadrer et régir (2).

CNP	Titre de la catégorie	Titres d'emploi illustratifs en cybersécurité[34]	Équivalent du cadre NICE[35]
0213	Gestionnaires des systèmes informatiques	• Directeur de l'intégration des technologies de l'information • Directeur des opérations de systèmes informatiques • Directeur en conception de réseaux	ER Encadrer et régir
2171	Analystes et consultants en informatique	• Analyste ou consultant en sécurité informatique • Planificateur de la sécurité des systèmes • Analyste en assurance de la qualité ou vérificateur de l'assurance de la qualité	SA Sécuriser l'approvisionnement
2172	Analystes de bases de données et administrateurs de données	• Architecte ou analyste de base de données • Analyste en système de traitement électronique des données • Administrateur de données	ER Encadrer et régir
2281	Techniciens de réseau informatique	• Technicien ou gestionnaire de réseau local • Administrateur réseau	ER Encadrer et régir
2283	Évaluateurs de systèmes informatiques	• Essayeur d'applications ou de logiciels • Technicien en essai de systèmes	SA Sécuriser l'approvisionnement

Figure 12 : Harmonisation des codes de la CNP en cybersécurité de Statistique Canada avec les catégories NICE selon une approche optimale en fonction des titres d'emploi similaires.

En harmonisant chaque source de données du Nouveau-Brunswick au cadre NICE, une tendance commune s'en dégage. Comme l'illustre la **figure 13**, le sondage mené auprès des employeurs souligne aussi la catégorie « Sécuriser l'approvisionnement ». Curieusement, les employeurs considèrent aussi la catégorie « Opérer et maintenir » comme importante. Bien que la catégorie « Encadrer et régir » semble moins importante, la plupart des répondants au sondage tombent eux-mêmes dans cette catégorie et pourraient simplement ne pas prévoir embaucher du personnel supplémentaire au sein de leur propre rôle.

[34]Les titres d'emplois de cette section sont tirés de la publication « Classification nationale des professions (CNP) 2011 » de Statistique Canada : https://www.statcan.gc.ca/fra/sujets/norme/cnp/2011/introduction.
[35]Déterminé en harmonisant les titres d'emplois en sécurité de Statistique Canada avec le supplément du cadre NICE : domaines de spécialité, rôles et tâches du cadre NICE, 2018.

Dans quelle mesure votre organisation a-t-elle besoin des rôles en cybersécurité suivants lorsque vous embauchez au Nouveau-Brunswick?

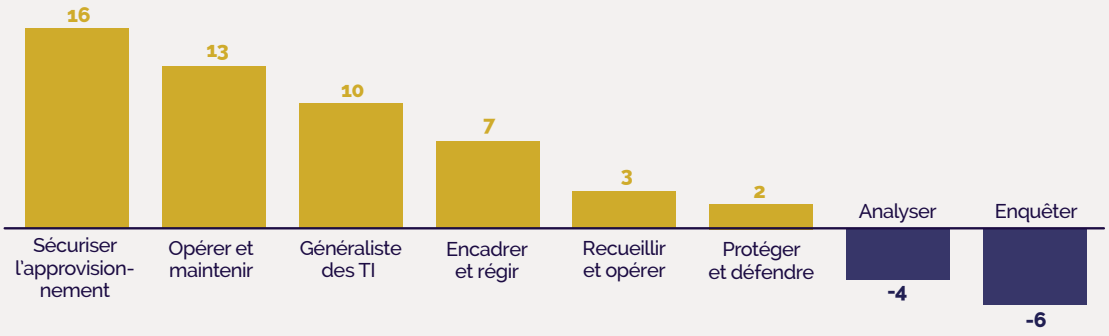
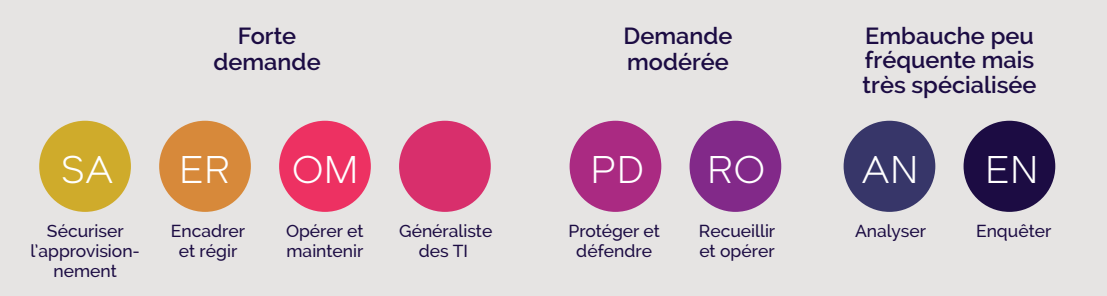


Figure 13 : Les employeurs du Nouveau-Brunswick ayant répondu au sondage recensent les rôles recherchés en cybersécurité dans la province. Dans le sondage, des descriptions de chaque rôle ont été présentées aux répondants, plutôt que la forme courte des catégories du cadre NICE énoncées ici. Source : CTIC, 2020 (chiffres calculés selon le classement des répondants : +2 « Demande urgente », +1 « Demande modérée », -1 « Aucune demande »).

En plus du sondage mené auprès des employeurs du Nouveau-Brunswick, de l'analyse de l'Enquête sur la population active et des entrevues auprès d'intervenants clés, le CTIC a relevé des avis d'emplois en cybersécurité dans la province pour guider son recensement des rôles recherchés. Le tableau suivant établit une vaste comparaison entre toutes les sources de données guidant la présente étude et le classement des compétences et des emplois recherchés en cybersécurité au Nouveau-Brunswick. Si les emplois sont classés approximativement dans le cadre NICE, il est possible de voir trois niveaux d'emplois recherchés. Bien qu'il existe une certaine variation selon la source, les rôles qui font partie de la catégorie « Sécuriser l'approvisionnement » sont clairement ceux les plus fréquemment annoncés, enregistrant de forts taux de croissance. Alors que les employeurs interrogés classent la catégorie « Opérer et maintenir » au deuxième rang, les données secondaires suggèrent que les rôles de grade supérieur de la catégorie « Encadrer et régir » sont également difficiles à trouver, et que les deux rôles rivalisent pour la deuxième place des emplois les plus recherchés. Par exemple, la plupart des emplois de la catégorie « Opérer et maintenir » sont dotés dans un délai d'un mois (comme le montre la **figure 14**), suggérant que ces emplois sont extrêmement difficiles à doter même si les organisations continuent d'embaucher ces professionnels. Un deuxième niveau de rôles, les catégories « Recueillir et opérer » et « Protéger et défendre », sont également moyennement recherchées, et les rôles des catégories « Analyser » et « Enquêter » (souvent hautement spécialisées) sont considérés comme parfois difficiles à doter, tout en étant moins fréquemment recherchés. De plus, plutôt que d'embaucher du personnel spécialisé, bon nombre d'organisations pourraient vouloir embaucher un généraliste des TI qui peut aussi contribuer à la cybersécurité.



Sondage auprès d'employeurs du N.-B.

Classés selon l'urgence

- Conseiller, architecte ou analyste de haut niveau en sécurité
- Rôle préventif responsable de l'administration de la gestion des risques, de la maintenance des systèmes et de la sécurité de l'infrastructure
- Généraliste des TI responsable de la cybersécurité
- Cadre de haut niveau en cybersécurité qui assure l'orientation, la gestion et la stratégie
- « Pirate éthique » qui vérifie la sécurité de l'infrastructure
- Gestionnaire d'incidents responsable de recenser les menaces et d'y répondre
- Scientifique des données, cryptographe ou analyste du renseignement
- Spécialiste de la criminalistique informatique responsable de recueillir des preuves numériques après un incident et d'identifier la source ou la nature de la menace

Entrevues auprès d'intervenants clés

Ordre sans importance – considérés comme les postes « les plus difficiles à doter au N.-B.

- Architectes de l'information et des systèmes
- Analyste de la sécurité
- Spécialistes de la sécurité infonuagique
- Développeurs de produits de cybersécurité en intelligence artificielle
- Ingénieurs en sécurité
- Administrateurs de la sécurité informatique
- Responsables de la gouvernance (risques et conformité)
- Agents principaux de cybersécurité
- Développeurs de logiciel (généraux)
- Vérificateurs des vulnérabilités et des intrusions
- Scientifiques des données
- Analystes en criminalistique informatique
- Chasseurs de menaces

Avis d'emplois au N.-B.

Par fréquence d'affichage, titres similaires agrégés

- Développeur de logiciels de sécurité
- Gestionnaire ou directeur en matière de gouvernance
- Architecte ou ingénieur en sécurité
- Analyste en assurance de la qualité en matière de sécurité
- Personnel du centre des opérations de sécurité
- Analyste en détection des incidents et intervention
- Analyste du renseignement
- Cyberopérateur

Enquête sur la population active

Selon le TCAM sur cinq ans au Nouveau-Brunswick

- Évaluateurs de systèmes informatiques
- Gestionnaires des systèmes informatiques
- Analystes et consultants en informatique
- Analystes de bases de données et administrateurs de données
- Techniciens de réseau informatique

Figure 14 : Emplois recherchés classés par ordre d'importance : Employeurs, analyste des avis d'emplois, Enquête sur la population active, entrevues auprès d'intervenants clés, catégorisés selon le cadre NICE.

Une ventilation détaillée des avis d'emplois en cybersécurité dans la province peut jeter davantage de lumière sur ces classements. La **figure 15** illustre deux conclusions clés quant aux types de rôles en cybersécurité annoncés au Nouveau-Brunswick : le nombre d'avis d'emplois par catégorie générale et le pourcentage des emplois dans chaque catégorie qui ont été dotés dans un délai d'un mois de leur affichage[36].

[36]Remarque : Cette analyse se fonde sur l'hypothèse voulant que l'avis soit supprimé lorsque l'emploi est doté. De plus, l'analyse suppose un emploi par avis unique, et qu'un avis d'emploi de la même entreprise, pour le même rôle, qui continue d'être affiché pendant plusieurs mois vise un seul poste plutôt que des demandes continues.

De plus, le nombre d'années d'expérience demandé (selon le chiffre minimum précisé lorsqu'une échelle était fournie) montre la variation entre ces catégories : il est clair que certains rôles exigent plus de spécialisation et d'expérience que d'autres, la plupart faisant partie des catégories « Sécuriser l'approvisionnement » et « Encadrer et régir ».

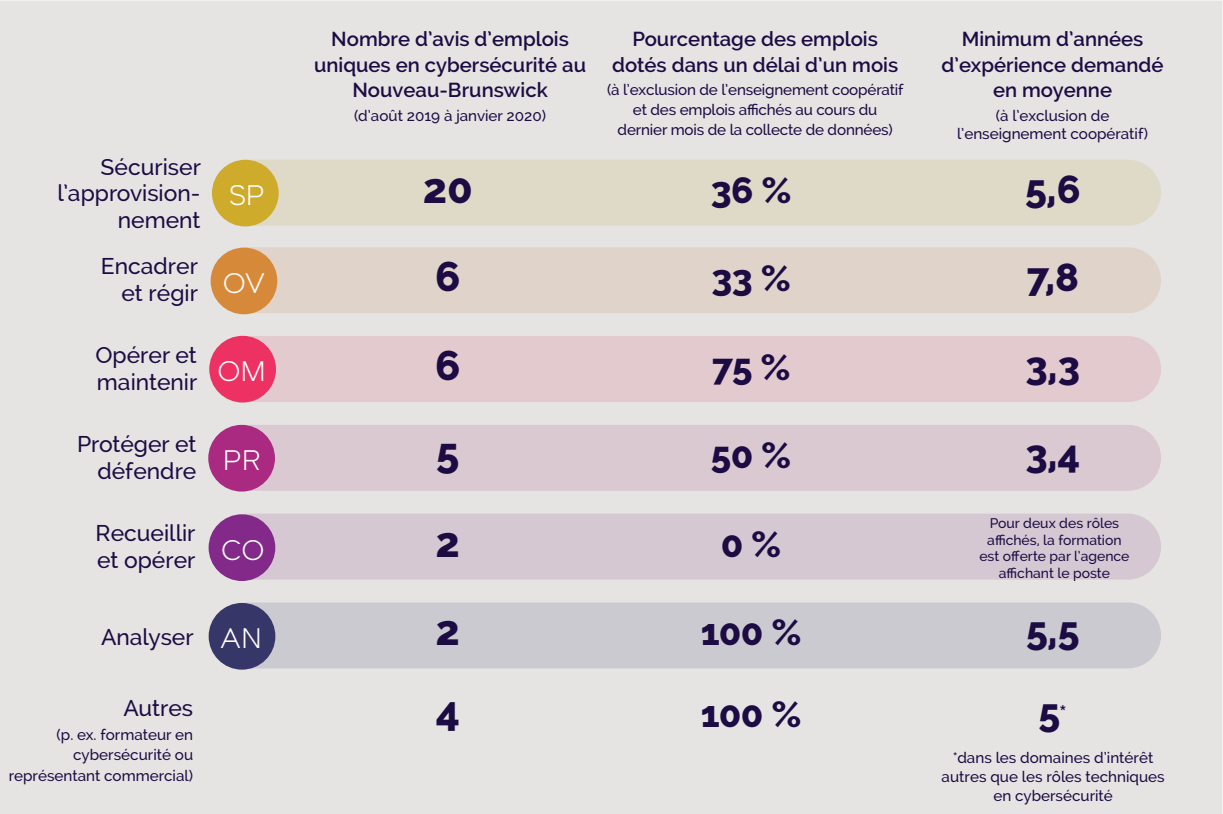


Figure 15 : Ventilation des avis d'emplois en cybersécurité au Nouveau-Brunswick, août 2019 à janvier 2020. Source : CTIC.

Compétences recherchées en cybersécurité

Comme plusieurs intervenants clés l'ont mentionné, les titres et les descriptions d'emplois dans l'écosystème de la cybersécurité ne sont pas toujours faciles à catégoriser puisque les employeurs rédigeront, assez régulièrement, des descriptions de travail très larges afin d'attirer des candidats des plus diversifiés. Ils ont aussi indiqué que les représentants de l'industrie saturent intentionnellement la liste des compétences exigées (autant humaines que techniques) des avis d'emplois puisqu'une liste de qualifications limitée ou stricte décourage souvent les candidats qualifiés. Les compétences sont donc propres à des rôles en particulier et, souvent, transversaux et s'appliquant à un vaste éventail de titres de postes. L'analyse ci-dessous inverse les compétences des moins précises aux plus précises, examinant d'abord les compétences humaines et transférables valorisées par les employeurs de deux façons : par des entrevues auprès d'intervenants clés et dans les descriptions de postes affichés.

Les compétences sont classées de façon générale selon l'ordre d'importance que les répondants leur ont attribué dans le cadre du sondage du CTIC mené auprès d'employeurs du Nouveau-Brunswick. Alors que les compétences varieront nécessairement considérablement selon le rôle, la comparaison et le classement suivants reflètent un certain degré d'importance transversale (surtout pour les compétences moins spécialisées) puisque les personnes interrogées et les répondants au sondage mentionnaient des compétences qui n'étaient pas liées à un titre de poste en particulier. Par conséquent, l'analyse de la **figure 16** constitue une vue d'ensemble des priorités des employeurs du Nouveau-Brunswick et des compétences transférables qui peuvent aider les candidats prometteurs à réussir.

En ce qui concerne les **compétences humaines et transférables**, les répondants au sondage ont classé la responsabilisation, le professionnalisme, le travail d'équipe et la communication comme étant les compétences les plus importantes. Étonnamment, ces multiples options de réponse s'avèrent beaucoup plus granulaires dans l'analyse des entrevues et du Web, les employeurs ciblant du personnel indépendant, expérimenté, dévoué et organisé. Cette insistance sur les professionnels expérimentés et responsables renforce la conclusion générale voulant que les employeurs cherchent fréquemment des candidats en cybersécurité qui possèdent plusieurs années d'expérience pertinente. De même, le travail d'équipe, les capacités interpersonnelles, la capacité d'adaptation et la flexibilité font partie des aspects considérés comme relativement importants dans le milieu de travail.

Alors que l'option à choix multiples du sondage quant à la « créativité » a obtenu un classement légèrement inférieur, les résultats découlant des entrevues et des avis d'emplois font la lumière sur les différences sémantiques à l'origine du problème : à la place de la « **créativité** », les employeurs en cybersécurité pourraient préférer des compétences en matière de **pensée critique**, d'**analyse**, de **résolution de problèmes** et de **réflexion stratégique**. De même, bien que le quotient émotionnel (c'est à-dire l'**empathie**) ne soit pas une réponse privilégiée dans le sondage, les employeurs ont volontairement mentionné des priorités entourant l'**intelligence émotionnelle** et la **connaissance situationnelle**, et le classement inférieur du leadership est contredit par l'importance du mentorat, du travail d'équipe, des compétences dans le domaine, de l'expérience antérieure et de la somme cumulative de bon nombre de ces compétences humaines qui, ensemble, créent un bon leader.

En plus des compétences humaines, la **figure 16** énumère les compétences techniques en cybersécurité qui ont été mentionnées pour chacune de ces sources de données. Les compétences sont regroupées et classées encore une fois selon l'importance que leur ont accordée les répondants au sondage. Nous avons demandé à deux professionnels ayant de l'expertise technique en cybersécurité de coder et de regrouper de façon indépendante les compétences de ces catégories, et leurs analyses ont été combinées (quoique grandement en accord) aux fins du tableau ci-dessous. Bien que ce tableau maintienne un fort degré de granularité, plusieurs conclusions sont claires. En particulier, plusieurs compétences sont systématiquement renforcées et utiles pour bon nombre de secteurs, notamment la sécurité des communications et des réseaux, l'ingénierie de sécurité, les concepts de protection, ainsi que l'architecture, la sécurité, les outils et les protocoles liés au réseau. Les deux codeurs ont mentionné qu'en raison de la combinaison de bon nombre de sources de données (avis d'emplois multiples et répondants multiples), il existait un important chevauchement de plusieurs des compétences énumérées ci-après. Cependant, la figure 16 conserve la formulation initiale de ces sources, dans la mesure du possible, afin de démontrer les demandes réelles des employeurs.

A Compétences humaines et transférables

Compétences classées par ordre d'importance selon le sondage mené par le CTIC auprès d'employeurs du Nouveau-Brunswick[37]	Compétences directement mentionnées dans les entrevues ou propres aux qualifications mentionnées dans les entrevues	Compétences tirées des avis d'emplois au Nouveau Brunswick (agrégées lorsque similaires)
1 Responsabilité et professionnalisme	• Motivé • Grande éthique professionnelle • Familiarité avec les systèmes d'entreprise • Passion ou intérêt pour la cybersécurité • Curiosité professionnelle	• Indépendance • Expérience dans un environnement d'entreprise • Gestion de projets
Travail d'équipe	• Collaboration et capacités interpersonnelles	• Compétences interpersonnelles • Mentorat, formation et renforcement des capacités pour les collègues
Communication	• Compétences en présentation • Compétences en communication (écrites et orales)	• Compétences en communication écrites et orales
2 Flexibilité	• Adaptabilité	• Gestion du temps et flexibilité
Créativité	• Aptitudes à la pensée critique	• Résolution de problèmes, analyse et pensée stratégique • Analyse des comportements humains
3 Courtoisie et empathie	• Intelligence émotionnelle (empathie) • Aptitudes au service à la clientèle	• Intelligence émotionnelle • Connaissance situationnelle • Service à la clientèle
Leadership	• Compétences en leadership • Expérience de bénévolat ou stage	• Compétences en leadership, gestion et supervision

[37]La question suivante a été posée aux répondants : « Lorsque vous embauchez du personnel en cybersécurité au Nouveau-Brunswick, quelles compétences (humaines ou techniques) parmi les suivantes sont les plus importantes? » Les groupes catégorisés sont fondés sur les classements des répondants, du plus important au moins important, les compétences dont les classements sont similaires ayant été regroupées. Ces questions du sondage ont reçu 40 réponses individuelles complètes.

B Compétences techniques propres à la cybersécurité

Compétences classées par ordre d'importance selon le sondage mené par le CTIC auprès d'employeurs du Nouveau-Brunswick[37]

Groupe un
(mieux classé dans le sondage)

- (A) Sécurité des réseaux
- (B) Connaissance de la sécurité infonuagique

Groupe deux
(deuxième rang)

- (C) Ingénierie des systèmes et réseaux
- (D) Intégration des technologies, systèmes et services
- (E) Sécurité de l'information et connaissance des pratiques exemplaires de l'architecture des systèmes
- (F) Gouvernance et conformité
- (G) Vérification des intrusions et des vulnérabilités
- (H) Enquête sur les incidents et intervention

Groupe trois

- (I) Évaluation et gestion des risques
- (J) Connaissance de la sécurité de l'Internet des objets
- (K) Chiffrement, cryptographie et cryptographie post-quantique

Compétences directement mentionnées dans les entrevues ou propres aux qualifications mentionnées dans les entrevues

- (A)(B)(C)(D)(E)(G)(H)(J)(K) Sécurité des communications et réseaux
- (C)(D)(E)(G)(H)(J) Gestion de l'identité et de l'accès
- (A)(C)(D)(E)(K) Ingénierie de sécurité
- (F)(G)(H)(I)(J) Analyse de la sécurité
- (F)(G)(H)(I) Vérification des systèmes d'information
- (F)(H)(I)(J) Gestion des risques
- (B)(H)(J) Sécurité infonuagique
- (C)(H) Opérations des systèmes d'information
- (D)(G) Sécurité du développement de logiciels
- (F)(H) Opérations de sécurité
- (G)(I) Security Assessment and Testing
- (F) Sécurité des biens
- (F) Acquisitions de systèmes d'information
- (F) Responsabilité de gestion
- (F) Gouvernance de la sécurité de l'information
- (H) Gestion des incidents
- (H) Chasse aux menaces

Compétences tirées des avis d'emplois au Nouveau Brunswick
(agrégées lorsque similaires)

- (A)(B)(C)(E)(F)(G)(H)(I)(J) Concepts de protection
- (A)(C)(D)(E)(G)(H)(J) Architecture, sécurité, outils et protocoles liés aux réseaux
- (D)(E)(H)(K) Protection et chiffrement des données
- (G)(H)(I)(J) Gestion et évaluation des vulnérabilités
- (G)(H)(I)(J) Analyse et évaluation des menaces
- (F)(H)(I) Gestion et atténuation des risques
- (A)(H) Gestion des pare-feu
- (E)(H) Automatisation (configuration, gestion, systèmes de sécurité
- (E)(H) Concepts et processus liés à la CNP
- (E)(H) Gestion des systèmes de sécurité d'entreprise
- (F)(I) Mesures et déclarations de sécurité
- (G)(K) Connaissance des méthodes d'attaque
- (F) Gouvernance et conformité
- (G) Vérification des intrusions
- (H) Surveillance des événements
- (H) Criminalistique numérique
- (H) Intervention en cas d'incident
- (H) Gestion des systèmes corrompus
- (H) Détection des intrusions complexes et perfectionnées
- (H) Élaborer des méthodes de chasse et de détection
- (H) Exécution des systèmes de prévention de la perte de données et de gestion des événements et de l'information de sécurité

C Autres compétences techniques

Compétences classées par ordre d'importance selon le sondage mené par le CTIC auprès d'employeurs du Nouveau-Brunswick[37]	Compétences directement mentionnées dans les entrevues ou propres aux qualifications mentionnées dans les entrevues	Compétences tirées des avis d'emplois au Nouveau Brunswick (agrégées lorsque similaires)
Compréhension des communications et des protocoles de réseau		• Administration et infrastructure des serveurs • Connaissance de la technologie mobile et de la radiotéléphonie
Développement de logiciels de base	• Programmation de base • Expérience de l'intelligence artificielle ou de l'apprentissage machine	• Méthodologies agiles • Programmation de base et avancée • Connaissance des structures de données et de mémoire
Cas particuliers (non catégorisés par les codeurs)	• Gestion de la TI • Documentation • Vérification et amélioration continue • Familiarité avec les systèmes d'entreprise (planification des ressources de l'entreprise)	• Administration des bases de données • Gestion des dossiers et des documents • Intégration et entreposage des données

** [réponses données à l'option ouverte « autre compétence importante (veuillez préciser) »]*

Perspectives des employeurs en matière de formation et d'éducation en cybersécurité

Les employeurs en cybersécurité au Nouveau-Brunswick expriment une préférence marquée pour le personnel ayant une grande expérience de travail, mais cette expérience se fonde sur la formation, qu'elle soit formelle, informelle, certification ou postsecondaire. Selon les répondants, bien que les qualifications académiques soient problématiques lorsque utilisées exclusivement, elles peuvent servir d'intermédiaires pour établir le profil des candidats qualifiés. La mesure dans laquelle les employeurs valorisent les différents types de formation et d'expérience se reflète globalement dans les conclusions du sondage exemplifiées à la **figure 17**.

Laquelle des qualifications suivantes est la plus importante?

Figure 17 : Qualifications classées par ordre d'importance dans le cadre du sondage mené par le CTIC auprès d'employeurs du Nouveau-Brunswick en cybersécurité. La question suivante a été posée aux employeurs : « Veuillez classer les options suivantes par ordre d'importance. Lorsque vous embauchez du personnel en cybersécurité, vous avez une préférence pour…? » (résultats attribués selon un classement pondéré).

La **figure 17** montre clairement que les employeurs valorisent davantage une formation concrète en cybersécurité (par le biais d'une expérience de travail antérieure en cybersécurité ou d'une certification propre à ce domaine comme un certificat professionnel) que des programmes d'études de base. Les employeurs ont pu faire la lumière sur cette question lors des entrevues, observant une tendance dans le paysage éducatif en cybersécurité qui tend à s'éloigner des diplômes traditionnels au profit des certifications professionnelles. Les répondants disaient préférer des candidats qui détiennent des certifications professionnelles, un thème récurrent, plusieurs commentant que les certifications reconnues par l'industrie (certifications CMPA, CISSP, SANS, etc.)[38] étaient fortement encouragées chez les talents potentiels, autant à l'échelle régionale qu'à l'étranger. Les organisations considéraient les certifications tout aussi importantes qu'une formation universitaire formelle, préférant même ces premières dans certains cas.

> *Dans l'ensemble, 60 % des employés de notre entreprise sont des informaticiens, alors que 40 % sont une combinaison de différents éléments ou détiennent une maîtrise dans un autre domaine, habituellement en biologie ou chimie. De toutes les personnes possédant une combinaison de différentes qualifications, certaines proviennent d'autres programmes universitaires, alors qu'environ un tiers d'entre elles détiennent diverses certifications et une grande expérience de travail.*
>
> – Adam Mosher, Global Intelligence Inc.

[38]*Les certifications des avis d'emplois affichés au Nouveau-Brunswick incluent les suivants (sans ordre particulier) : TOGAF, SABSA, ITIL, ISSAP, ISEP, CISA, CISSP, GCFA CEH, ISACA Cybersecurity Fundamentals Certification, ISA, NIST, CISM, CGEIT, CRISC, CBCP, PCIP, ISO27001, CCNA, MCSE, Security+, C|CISO, GIAC, CBCP, CIPP/C, SANS, COBIT, Agile, FIPS, STIG.*

Comme le mentionne une précédente citation, dans certains cas, les entreprises de cybersécurité embauchent des employés qui ne semblent pas détenir de diplôme pertinent, les candidats n'ayant pas ou guère de formation formelle. Une des personnes interrogées a indiqué qu'environ 50 % de sa main-d'œuvre était composée de personnes ayant une formation universitaire formelle, alors que l'autre moitié est autodidacte ou possède diverses certifications en matière de sécurité.

> *Nous avons embauché un homme au début de la trentaine, un chef, un passionné de cybersécurité. Il s'est avéré être l'un de nos meilleurs vérificateurs des intrusions, sans même avoir de compétences formelles. Il était seulement incroyablement autodidacte. Il s'est avéré un monstre sacré dans le domaine.*
>
> – Andrew Jefferies, Deloitte, anciennement Bulletproof

Malgré cette perspective, les avis d'emplois en cybersécurité continuent d'exiger que les candidats possèdent des diplômes de premier cycle ou d'études supérieures dans des domaines traditionnellement liés à la cybersécurité : l'informatique, l'ingénierie (généralement électrique ou logiciel), les TI, les systèmes d'information, le réseautage, l'automatisation, ou un autre domaine connexe. Certains postes de haut niveau, en gestion ou liés aux interactions avec les clients exigeaient aussi une maîtrise en administration des affaires.

Les personnes interrogées ont également mentionné que le réseau de collèges de la province, en plus de sa rapidité et de sa souplesse à demeurer réceptif à la rétroaction de l'industrie, était perçu d'une façon très positive. La capacité de s'assurer que le contenu demeure pertinent et qu'une formation moderne utilisant des produits novateurs soit offerte était intéressante. Les représentants de l'industrie encourageaient fortement la province à continuer d'uniformiser et de renouveler les programmes en cybersécurité en raison de la nature dynamique et fluide de l'industrie.

Plusieurs entreprises de cybersécurité du Nouveau-Brunswick embauchent régulièrement des stagiaires ou des étudiants en enseignement coopératif qui sont encore à l'école ou qui viennent tout juste de terminer leurs études. Les candidats ayant pratiqué des activités parascolaires ont priorité pour ce type de rôle : les expériences de bénévolat et la participation à des activités communautaires[39] étaient considérées comme des initiatives de réseautage et de renforcement des compétences.

Un processus de recrutement mystérieux : le marché du travail caché et l'acquisition de talents

Dans un domaine où il est normalement difficile de trouver des talents qualifiés, la capacité de repêcher des candidats qui possèdent une formation précise ou spécialisée est encore plus complexe. Sans l'arrivée massive de professionnels expérimentés, la capacité de développer une entreprise dans un secteur où la demande est forte présente des difficultés qui ont un impact sur la croissance et le potentiel économique.

[39] *Comme le programme CyberTitan mentionné précédemment*

Ces difficultés se traduisent souvent par le recrutement de talents qualifiés non pas à partir du bassin de talents disponibles, mais auprès d'autres talents employés ailleurs. Par conséquent, selon les consultants de l'industrie au Nouveau-Brunswick, même si les avis d'emplois pouvaient représenter des tendances en matière d'embauche, ils ne sont probablement pas un reflet exact du nombre absolu d'emplois réellement disponibles. Plusieurs emplois ne sont probablement pas annoncés, bon nombre des répondants admettant qu'ils affichaient parfois un emploi en dernier recours.

> *Je demande à des partenaires de l'industrie s'ils connaissent quelqu'un qui se cherche du travail parce que nous voulons embaucher pour un poste en particulier. Habituellement, j'attends une ou deux semaines pour voir si je vais recevoir des réponses à ma demande. Dans le cas contraire, nous empruntons la voie plus traditionnelle. Nous demandons aux universités si de futurs diplômés se cherchent du travail. Nous demandons même aux grands fabricants de logiciels s'ils connaissent quelqu'un qui envisagerait de quitter leur organisation. Généralement, les conversations sont très intéressantes. Au bout du compte, si aucune de ces méthodes n'est pas fructueuse, nous nous tournerons vers Indeed ou Career Beacon.*
>
> – Adam Mosher, Global Intelligence Inc.

Le marché du travail caché est le symptôme d'un écosystème très bien réseauté composé de différentes connexions personnelles, et offre des avantages supplémentaires, notamment en préservant la confidentialité des secrets organisationnels (p. ex. nouveaux domaines de recherche et développement, services aux entreprises, etc.) ou en recensant des talents de plus fort calibre qui occupent un emploi à temps plein ailleurs.

Raisons justifiant la demande en cybersécurité au Nouveau-Brunswick et au Canada

> *Nous devons absolument rivaliser avec les grandes sociétés comme IBM et Microsoft qui sont en mesure de verser des salaires élevés. Nous ne pouvons pas mobiliser ce type de fonds alors nous recrutons des jeunes hommes et femmes qui sortent de l'université, qui ont en moyenne 23 ou 24 ans, et nous les payons généralement entre 85 000 et 95 000 $ par année. Nous leur offrons de 4 à 5 semaines de vacances, un régime complet d'assurance-maladie et dentaire, en plus de certains autres avantages. C'est notre façon de compenser puisque nous ne pouvons pas leur offrir des salaires de 125 000 à 140 000 $ comme le font les grandes sociétés.*
>
> – Adam Mosher, Global Intelligence Inc.

Les pénuries de main-d'œuvre découlent souvent d'une combinaison complexe de variables : dans la recherche existante sur la demande de professionnels en cybersécurité, les employeurs ont précisé une vaste gamme de raisons pour les difficultés auxquelles ils font face en matière d'embauche, notamment les lacunes en matière de compétences, le maintien en poste, les parcours professionnels vagues, les attentes salariales et la diversité. Dans le cadre du sondage du CTIC auprès des employeurs, les répondants ont été invités à préciser les difficultés auxquelles ils ont dû faire face. Étonnamment, alors que la principale difficulté semble être de dénicher du personnel qualifié (un problème rencontré par près du tiers des employeurs), seulement 11 % des répondants estimaient que le problème pouvait être attribuable à la pénurie de candidats en cybersécurité dans la province en général, laissant entendre que les pénuries de main-d'œuvre dans le domaine au Nouveau-Brunswick sont propres aux postes très spécialisés. De plus, les salaires élevés et l'absence de parcours professionnels clairs pour les récents diplômés sont également des problèmes rencontrés par environ un cinquième (22 % et 17 %, respectivement) des employeurs.

Auquel des défis d'embauche en cybersécurité suivants avez-vous dû faire face au N.–B.?

% d'employeurs ayant fait face à ce défi

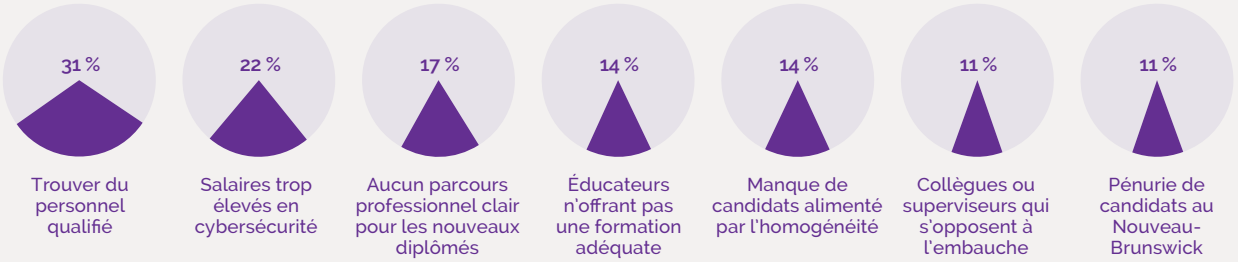


Figure 18: Perspectives des employeurs quant aux difficultés en matière d'embauche au Nouveau-Brunswick. Remarque : Les réponses au sondage ont été condensées ici pour en faciliter la lecture. Sondage du CTIC auprès d'employeurs en cybersécurité au Nouveau-Brunswick, 2019

La littérature nationale et internationale vient renforcer les expériences des employeurs du Nouveau Brunswick. En général, les talents qualifiés et expérimentés sont difficiles à trouver. Dans le cadre d'une étude canadienne réalisée en 2018 par Deloitte, la grande majorité des responsables principaux de la sécurité de l'information ont précisé qu'il était très difficile de recruter un candidat en cybersécurité possédant la bonne combinaison de compétences techniques, analytiques et générales (76 %)[40]. ISACA, une organisation internationale de cybersécurité, a également sondé des organisations sur la question, et la plupart des employeurs estimaient que la majorité des candidats en cybersécurité n'étaient pas qualifiés pour les postes qu'ils convoitaient[41]. Les salaires élevés en cybersécurité représentent aussi un défi presque universel pour les entreprises. Les salaires élevés en cybersécurité représentent aussi un défi presque universel pour les entreprises. Un tiers des responsables principaux de la sécurité de l'information estimaient que les régimes de rémunération dans le domaine sont gonflés en raison de la demande[42], et en Amérique du Nord, cette opinion est affirmée par 41 % des répondants[43].

[40]Deloitte and Toronto Financial Services Alliance. The changing faces of cybersecurity: Closing the cyber risk gap, 2018, p. 12-14.
[41]ISACA. State of cybersecurity 2019: Current trends in workforce development, 2019, p. 8.
[42]Deloitte and Toronto Financial Services Alliance. The changing faces of cybersecurity: Closing the cyber risk gap, 2018, p. 12-14.
[43]Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, p. 4.

Au Canada, 27 % des entreprises interrogées par l'ACEI ont indiqué qu'elles ne disposaient pas des ressources nécessaires pour employer un professionnel en cybersécurité, et celles qui embauchaient des consultants externes dans le domaine y consacraient en moyenne 19 % de leur budget total en TI[44].

Comme nous le verrons dans la section sur l'approvisionnement, le secteur de la cybersécurité manque de diversité. Alors que seulement quelques-uns (15 %) des employeurs interrogés au Nouveau Brunswick ont dénoté que l'homogénéité fondée sur l'origine ethnique et le sexe était un problème, il pourrait exister un bassin inexploité de nouveaux arrivants sur le marché du travail. En ce qui concerne la disparité de genre liée aux possibilités offertes, ISACA a constaté que seulement 41 % des femmes en cybersécurité estimaient que les femmes se voyaient offrir les mêmes options d'avancement professionnel que les hommes (comparativement à 79 % des répondants masculins)[45]. Mondialement, en 2016, les femmes en cybersécurité ont gagné moins que les hommes à tous les échelons d'emploi[46], même si les femmes intègrent généralement le domaine en ayant atteint de meilleurs niveaux de scolarité que les hommes[47]. Les responsables principaux de la sécurité de l'information ont mentionné la sous-représentation des femmes comme facteur contribuant au faible nombre de professionnels expérimentés en cybersécurité[48].

[44]ACEI. Sondage sur la cybersécurité, automne 2018, p. 10.
[45]ISACA. State of cybersecurity 2019: Current trends in workforce development, 2019, p. 14.
[46]Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, p. 5.
[47]Ibidem, p. 10.
[48]Deloitte and Toronto Financial Services Alliance. The changing faces of cybersecurity: Closing the cyber risk gap, 2018, p. 12-14.

COMPRENDRE L'OFFRE DE MAIN-D'ŒUVRE EN CYBERSÉCURITÉ

au Canada et au Nouveau Brunswick

Nous voulons bâtir la communauté ici [au Nouveau-Brunswick] parce que nous en faisons partie, et c'est important. Notre processus de recrutement doit s'harmoniser avec notre croissance. Il est difficile de trouver, d'attirer et de garder des talents qualifiés dans ce secteur. Il est donc logique d'intégrer le plus d'avenues possible dans l'équation. Nous ciblons autant la maternelle à la 12e année que l'enseignement coopératif universitaire, et nous embauchons beaucoup de nouveaux immigrants.

. – Andrew Jefferies, Deloitte, anciennement Bulletproof

Données démographiques dans le secteur de la cybersécurité

Tant au Nouveau-Brunswick que dans le reste du monde, le secteur de la cybersécurité manque de diversité, entraînant de graves conséquences en ce qui concerne le bassin disponible de personnel qualifié. Cette tendance touche aussi le Nouveau-Brunswick, comme en témoignent les estimations des employeurs interrogés quant au nombre de femmes, de Canadiens de première génération, d'Autochtones, de membres des minorités visibles et de personnes handicapées faisant partie de leur main-d'œuvre en cybersécurité (voir la **figure 19**). Par exemple, plus de la moitié (52 %) des employeurs interrogés au Nouveau-Brunswick indiquent que leur main-d'œuvre en cybersécurité ne compte aucune femme, alors qu'un tiers (34 %) d'entre eux emploient une main-d'œuvre entièrement de race blanche.

Diversity of Cybersecurity Personnel in Cybersecurity Respondents' Workplaces

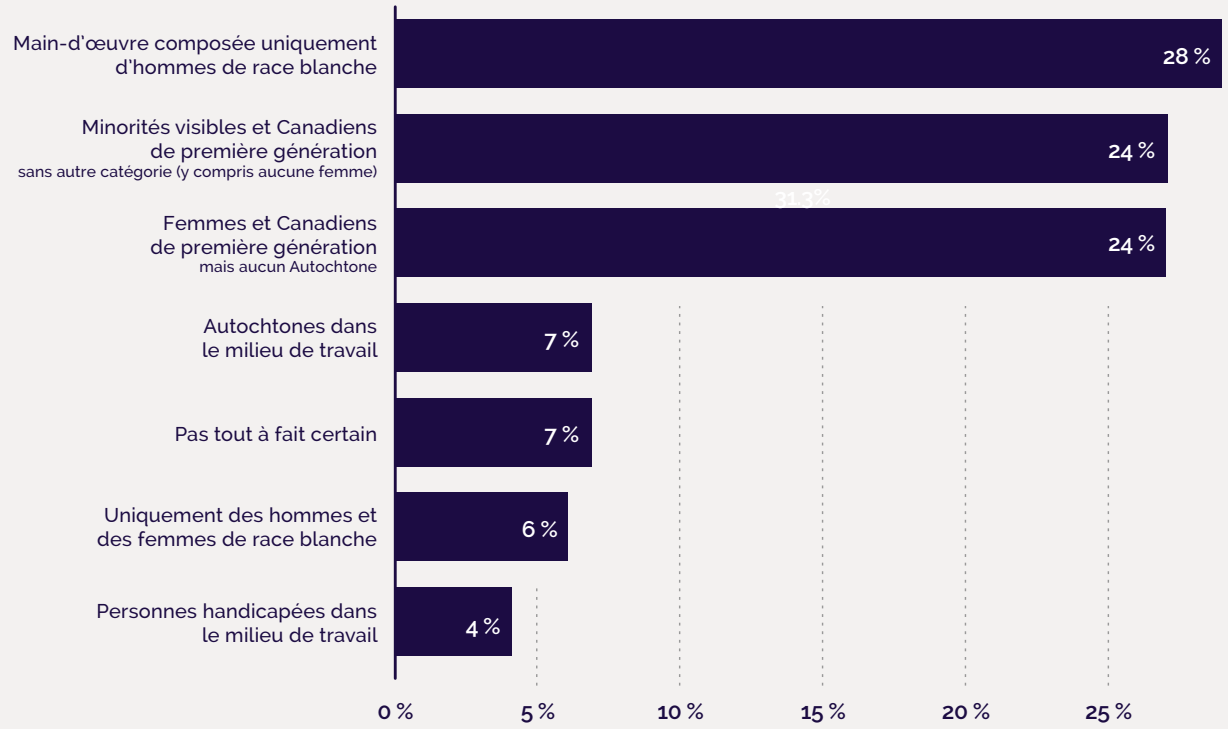


Figure 19 : Composition de la main-d'œuvre en cybersécurité au Nouveau-Brunswick.
Sondage du CTIC auprès d'employeurs en cybersécurité du Nouveau-Brunswick.

La prochaine section examine les tendances démographiques dans la province et globalement, surtout en ce qui concerne la main-d'œuvre en cybersécurité.

Genre

À l'échelle internationale, environ 11 % de la main-d'œuvre en cybersécurité est composée de femmes[49]. Alors que ce taux est de 14 % en Amérique du Nord, la plus grande concentration régionale au monde, les femmes demeurent tout de même considérablement sous-représentées en cybersécurité[50]. De plus, les hommes sont 4 fois plus susceptibles d'occuper des postes de cadres et de dirigeants, et 9 fois plus susceptibles d'occuper des postes de gestion, que les femmes en Amérique du Nord[51]. Selon une étude américaine, bien que les minorités ethniques soient représentées de façon proportionnelle dans le secteur de la cybersécurité, elles sont également moins susceptibles d'occuper des postes supérieurs, et les femmes de couleur en particulier sont sous-payées de près de 10 000 $ en moyenne, comparativement à leurs collègues masculins blancs de même statut[52].

À l'échelle provinciale, la **figure 20** montre que les femmes représentent un nombre démesurément petit de la main-d'œuvre en cybersécurité du Nouveau-Brunswick et qu'elles sont moins nombreuses à occuper des rôles de gestion offrant des salaires moyens supérieurs, alors que seulement 22,5 % des gestionnaires des systèmes informatiques s'identifiaient comme des femmes en 2015.

Genre et salaire moyen en cybersécurité au Nouveau-Brunswick

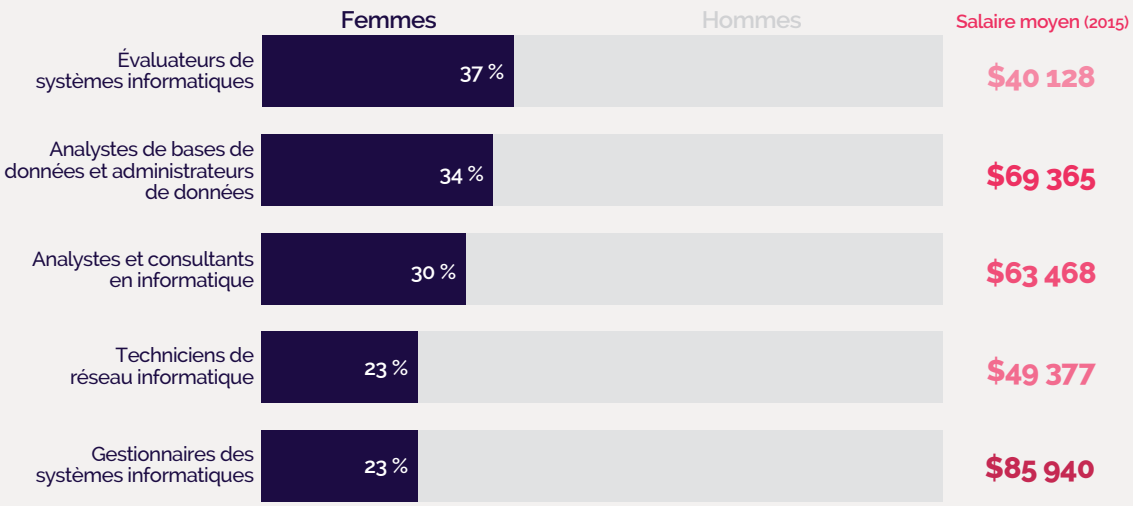


Figure 20 : Genre et salaire moyen des emplois en cybersécurité de la CNP au Nouveau-Brunswick, 2015. Source : Gouvernement du Nouveau-Brunswick, www.nbjobs.ca

[49] *Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Women in Cybersecurity, Frost & Sullivan, 2017 : https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf, p. 6.*
[50] *Ibidem.*
[51] *Ibidem, p. 5.*
[52] *Ibidem.*

Âge et salaire

De même, comme le montre la figure 21, les salaires en cybersécurité tendent à augmenter pour les postes occupés par des groupes d'employés proportionnellement plus âgés. Le rôle enregistrant le plus grand nombre de jeunes employés, les évaluateurs de systèmes informatiques, enregistrait le salaire moyen le moins élevé, soit 40 128 $ en 2015. Cette tendance pourrait être liée à l'éducation puisque les deux emplois offrant les plus bas salaires sont aussi les moins susceptibles de nécessiter un diplôme universitaire parmi les cinq rôles énumérés dans la figure. Aussi, la main-d'œuvre du Nouveau Brunswick enregistre un âge moyen légèrement plus élevé qu'au Canada (43,6 % comparativement à 41,0 % au Canada en 2016)[53]. Tandis que le Canada connaît une hausse de l'âge moyen, les soins de santé permettant de prolonger la vie et les taux de fertilité étant à la baisse, le Nouveau Brunswick vit cette transition encore plus rapidement. L'âge moyen au Canada a augmenté de 0,9 année de 2011 à 2016, et de 1,5 année au Nouveau-Brunswick[54]. De plus, le secteur des technologies de la province rajeunit : par exemple, en date de décembre 2019, 43 % de la main-d'œuvre totale du Nouveau-Brunswick avait entre 45 et 64 ans, comparativement à seulement 35 % de la main-d'œuvre dans le secteur des technologies[55]. À ce titre, la démographie unique de la province suppose la nécessité d'établir des parcours professionnels clairs pour que les jeunes travailleurs commencent à occuper des emplois plus spécialisés et mieux rémunérés, ainsi que des mesures pour retenir les jeunes dans la province.

Âge et salaire moyen en cybersécurité au Nouveau-Brunswick

2015, dollars canadiens

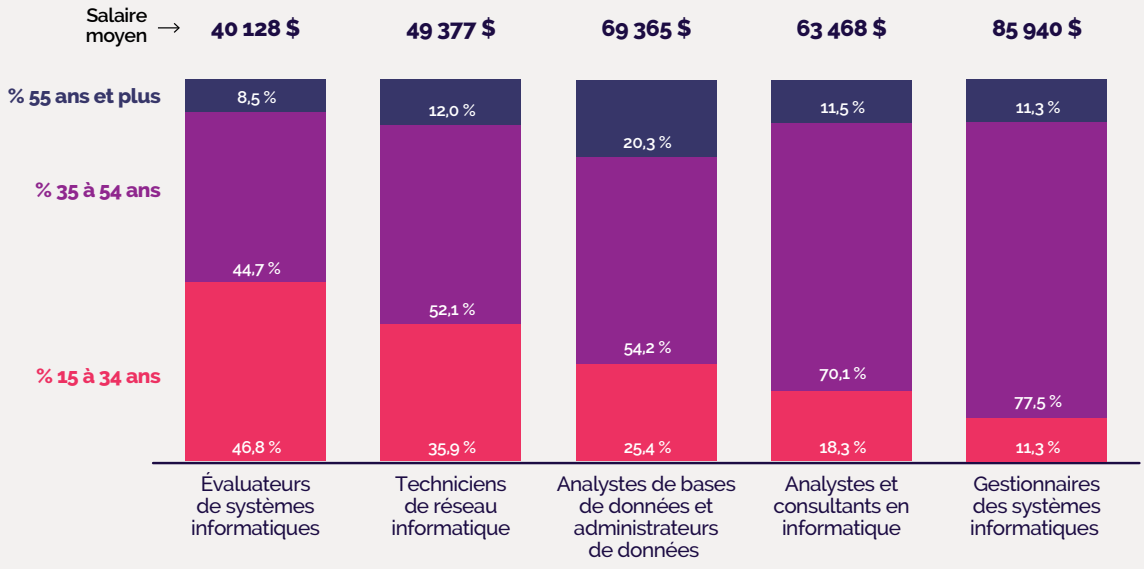


Figure 21 : Âge et salaire moyen de la main-d'œuvre en cybersécurité au Nouveau-Brunswick (2015, dollars canadiens). Source : Gouvernement du Nouveau-Brunswick, emploisNB.

[53] *Statistique Canada, 2016.*
[54] *Gouvernement du Nouveau-Brunswick, 2016.*
[55] *Statistique Canada, 2019.*

Autochtones

Les personnes interrogées ont fait remarquer que la main-d'œuvre autochtone du Nouveau-Brunswick avait connu une croissance appréciable en raison des changements touchant l'auto-identification (un changement de culture positif), de la croissance démographique naturelle et de la migration d'entrée. Toutefois, il demeure des lacunes en matière d'éducation (les Autochtones étant moins susceptibles de détenir un diplôme d'études postsecondaires), de rémunération et d'autres indicateurs sociaux importants. En se fondant sur la petite taille du secteur de la cybersécurité, le pourcentage relativement faible de Néo-Brunswickois qui s'identifient comme Autochtones (4 % en 2016)[56], et les formidables obstacles à l'entrée comme le lieu et l'accès aux centres urbains, il y a probablement peu d'Autochtones employés en cybersécurité dans l'ensemble du Nouveau-Brunswick. Environ 90 % des employeurs interrogés ont confirmé que leur industrie n'employait aucun Autochtone s'identifiant comme tel, comme le montre la figure 19. Les organismes de perfectionnement de la main-d'œuvre, sujet abordé dans une prochaine section, cherchent à combler cette lacune et à rendre le domaine de la cybersécurité, ainsi que ces emplois convoités et bien rémunérés, plus accessible aux Autochtones de la province.

Nouveaux arrivants et immigrants

Les nouveaux arrivants au Canada représentent une partie importante de la main-d'œuvre en technologie au pays. Alors qu'il existe peu de données sur la composition nationale de la main-d'œuvre en cybersécurité au Nouveau-Brunswick, les questions sur les nouveaux arrivants et les immigrants au Nouveau-Brunswick ont reçu un accueil mitigé de la part des personnes interrogées. Certains répondants ont parlé des difficultés relatives aux autorisations de sécurité en dehors du Groupe des cinq pour les experts hautement qualifiés. Une des personnes interrogées a souligné d'autres obstacles en matière d'autorisations de sécurité concernant les visas des travailleurs assignés à des projets de clients américains. Un autre chef de file de l'industrie croit que tous les talents internationaux (en dehors du Groupe des cinq) assignés à travailler auprès d'entreprises américaines rencontreraient probablement des obstacles à l'obtention de visas de voyage temporaire en raison des préoccupations en matière de sécurité. D'autres répondants ont précisé que le manque historique de diversité ethnique dans la province représente un obstacle permanent pour les nouveaux arrivants. Les difficultés associées aux contacts et aux communications à distance ainsi qu'aux processus d'immigration entraînent un long processus de recrutement.

> *Le processus d'embauche de candidats internationaux prend beaucoup plus de temps au Nouveau-Brunswick. Plutôt que de prendre deux semaines, le processus prend deux mois, quatre mois ou même plus.*
>
> – Anonyme

[56] *Statistique Canada, 2019.*

Cependant, les répondants ont souligné un virage croissant de la culture de l'industrie, précisant que la pénurie de talents nationaux qualifiés obligeait les gestionnaires recruteurs à se tourner vers l'étranger pour trouver des solutions de qualité. Certaines organisations ont également signalé que leurs pratiques efficaces d'embauche internationale constituaient un atout pour leur main-d'œuvre actuelle. Les répondants ont souligné la valeur de milieux de travail diversifiés sur le plan culturel dans le domaine de la cybersécurité puisqu'ils permettent de mieux comprendre les défis uniques en matière de sécurité. À leur avis, les perspectives internationales pourraient apporter des éclaircissements quant aux motivations et aux méthodes de divers auteurs de menaces.

Les organisations interrogées ont eu l'occasion de préciser le lieu d'origine de leurs talents internationaux. En plus des États-Unis et de l'Union européenne, ils ont identifié plusieurs pays, notamment le Nigéria, les Philippines, l'Inde, les Émirats arabes unis, le Mexique, le Venezuela, la Corée du Sud et l'Égypte. Entre 2011 et 2016, la population du Nouveau-Brunswick a diminué de 0,5 %, alors que le Canada dans son ensemble a connu une hausse de 5 %[57]. Cette disparité signale la nécessité de diversifier le bassin de population de la province, et le programme d'immigration[58] pourrait être un moyen de profiler des talents internationaux qui peuvent soutenir la croissance de l'industrie.

Programmes éducatifs en cybersécurité au Nouveau-Brunswick

Globalement, la plupart des professionnels en cybersécurité obtiennent d'abord un diplôme en informatique ou génie informatique et bon nombre font une transition dans leur domaine depuis une ancienne carrière en TI, finances, défense, marketing, commerce, comptabilité ou dans d'autres industries55. La province du Nouveau-Brunswick offre une variété de programmes académiques visant à former des diplômés en cybersécurité, et ces efforts commencent à l'école primaire. La liste ci-dessous énumère les programmes de cybersécurité et les efforts de perfectionnement de la main-d'œuvre au Nouveau-Brunswick de l'école primaire au niveau postsecondaire mentionnés par les répondants au sondage, mais se veut davantage illustrative qu'exhaustive.

École primaire à secondaire : Les répondants ont indiqué qu'une grande variété de matériel lié à la cybersécurité est incluse dans le programme de la maternelle à la 12e année au Nouveau Brunswick, en partie grâce au partenariat entre CyberNB et le ministère de l'Éducation et du Développement de la petite enfance. Ils ont mentionné que plusieurs pays chefs de file du secteur de la cybersécurité, comme Israël, voyaient l'intégration académique du Nouveau Brunswick à la cybersécurité de façon favorable et la considéraient comme un exemple international.

[57]Statistique Canada, 2019.
[58]Les exemples de programmes efficaces potentiels d'immigration incluent le programme GO Talent du CTIC : https://www.ictc-ctic.ca/programmes-des-talents/?lang=fr

Programmes postsecondaires de certificat et à court terme en cybersécurité :

Le Collège communautaire (francophone) du Nouveau-Brunswick offre un programme en cybersécurité de 80 semaines, dont un stage qui traite de cryptologie, de gestion des risques, de piratage éthique, de programmation Java et Python, de sécurité des applications, des bases de données, de réseaux et de systèmes. Le programme cherche précisément à former des travailleurs pour des postes d'analystes et de consultants en informatique (CNP 2171)[59].

L'Université francophone de Moncton offre un certificat de 8 cours (24 crédits) en sécurité de l'information des entreprises, dont environ la moitié cible des sujets liés à la cybersécurité[60].

Le Collège communautaire (anglophone) du Nouveau-Brunswick offre un diplôme d'études avancées d'un an en cybersécurité. Le programme inclut 14 cours liés à la cybersécurité abordant des sujets comme la gestion des risques, la sécurité des points d'accès, le piratage éthique, les interventions en cas d'incident, la criminalistique, la sécurité humaine et logicielle, et les produits de sécurité d'entreprise. Il vise surtout à former des analystes et des consultants en informatique (CNP 2171) et des techniciens de réseau informatique (CNP 2281)[61].

L'établissement privé Outlon Collège offre un programme en cybersécurité et gestion des systèmes de 10 mois qui se conclut par un stage de 4 semaines. Le programme cible la gestion des systèmes plutôt que la cybersécurité et n'inclut aucune formation en programmation Java ou Python[62].

L'établissement privé Eastern College offre un programme de 81 semaines en gestion avancée des systèmes et cybersécurité qui vise des postes de techniciens de réseau informatique (CNP 2281) et d'agents de soutien aux utilisateurs (CNP 2282). Le programme se termine par un stage pratique de 16 semaines[63].

Options propres à la cybersécurité au baccalauréat : L'Université du Nouveau-Brunswick offre une option pour se spécialiser en cybersécurité dans le cadre du programme de baccalauréat en informatique[64]. La spécialisation en cybersécurité compte 12 crédits et inclut un cours en sécurité logicielle et criminalistique numérique ainsi qu'un projet intégrateur de 6 crédits qui comprend une thèse[65]. Les étudiants peuvent aussi participer à un programme d'enseignement coopératif. De plus, plusieurs établissements postsecondaires de la province, dont Mount Allison, offrent des cours individuels pour acquérir des compétences en cybersécurité, comme la cryptographie, en tant qu'options de cours pour les étudiants en informatique, mathématiques ou ingénierie.

[59]CCNB. « Cybersecurity ». Nos programmes : https://ccnb.ca/programme-detudes/nos-programmes.aspx?SectorId=9417243f-3b20-42ed-91de-82bb281c8134&ObjectType=1&Id=b3ae566b-d545-4212-a8da-b386d7184913
[60]Université de Moncton. « Bachelor in Information Management » : https://www.umoncton.ca/umcs-bgi/node/55
[61]CCNB. « Information Technology: Cybersecurity » : https://nbcc.ca/programs-courses/program-details?baseCurriculumId=dd3a4616-5e03-4a27-b585-d074efdd4178
[62]Oulton College. « Systems Management and Cybersecurity » : https://oultoncollege.com/systems-management-and-cybersecurity/
[63]Eastern College. « Advanced Systems Management and Cybersecurity » : https://www.easterncollege.ca/programs-courses/technology/advanced-systems-management-and-cybersecurity/
[64]Université du Nouveau-Brunswick. « Areas of Specialization » : https://www.unb.ca/fredericton/cs/undergrad/bcs/specialization.html
[65]Ibidem.

Études supérieures : L'Université du Nouveau-Brunswick offre une maîtrise en cybersécurité appliquée. Ce programme d'un an comprend neuf cours (y compris des laboratoires informatiques) et un projet intégrateur en recherche et développement auprès d'un partenaire de l'industrie. Les diplômés du programme peuvent acquérir une expérience supplémentaire par le biais d'études permettant d'acquérir des connaissances en cybersécurité à fort coefficient de recherche, un complément qui dure quatre mois et qui commence tout de suite après l'obtention du diplôme. Les quatre mois additionnels incluent des modèles en gestion de projets de cybersécurité et de développement de produits, ainsi qu'une expérience de travail supplémentaire auprès d'un partenaire de l'industrie[66].

Programmes auxiliaires :

Le programme de formation en cybersécurité de l'Initiative conjointe de développement économique est une initiative de formation à l'emploi offert aux Autochtones du Nouveau-Brunswick. Le 19 juillet 2019, six apprenants participant au programme ont obtenu une certification en cybersécurité du Collège communautaire (anglophone) du Nouveau-Brunswick[67].

L'Institut canadien sur la cybersécurité de l'Université du Nouveau-Brunswick offre le cours Cybersécurité 101, une formation intensive de 4 jours en cybersécurité pour les professionnels en TI de l'extérieur du domaine. Le cours inclut des exposés magistraux, des laboratoires, des activités et des démonstrations. Il offre un aperçu des risques pour la cybersécurité, des pratiques de gestion des risques, des mesures de prévention et de détection des intrusions, et des interventions en cas d'incidents[68].

Comme l'illustre la liste exhaustive de programmes mentionnés dans le présent rapport, le Nouveau Brunswick est manifestement un carrefour d'éducation en cybersécurité dans le Canada atlantique. À l'échelle nationale, la province va au-delà de son poids démographique en ce qui concerne son offre éducative, alors que quatre établissements postsecondaires publics offrent des programmes en cybersécurité. À cet égard, la province se classe au quatrième rang au Canada, derrière l'Ontario, le Québec et l'Alberta. Le Nouveau-Brunswick est l'une des trois provinces à offrir une maîtrise en cybersécurité (les deux autres étant l'Ontario et le Québec). L'offre éducative du Nouveau-Brunswick en cybersécurité est particulièrement impressionnante si l'on tient compte des provinces du centre et de l'ouest du Canada. Le Nouveau-Brunswick offre environ la moitié des programmes universitaires en cybersécurité qu'offre le Québec, et environ le quart de ce que propose l'Ontario, mais les populations de ces deux provinces sont plus de 10 fois celle du Nouveau-Brunswick. Les programmes collégiaux et universitaires du Nouveau-Brunswick sont comparables à ceux des provinces les plus populeuses de l'Ouest.

Le Nouveau-Brunswick est reconnu comme un carrefour en cybersécurité même par les grandes entreprises internationales. L'Université du Nouveau-Brunswick, qui héberge l'Institut canadien sur la cybersécurité, est l'une des huit universités en Amérique du Nord (dont trois au Canada) choisie par IBM pour travailler sur le projet Watson, une technologie de cybersécurité cognitive[69].

[66]Université du Nouveau-Brunswick. « Experiential Addendum: Research Intensive Cyber Knowledge Studies (RICS) » : https://www.unb.ca/fredericton/cs/grad/masters/macsec/rics.html
[67]Bulletproof. « The Joint Economic Development Initiative Announces the Graduation of the Inaugural Cohort of Indigenous Cybersecurity Professionals » : https://www.bulletproofsi.com/blog/the-joint-economic-development-initiative-announces-the-graduation-of-the-inaugural-cohort-of-indigenous-cybersecurity-professionals/
[68]Université du Nouveau-Brunswick. « Cybersecurity 101 » : https://www.unb.ca/cic/cybersecurity-101.html
[69]Université du Nouveau-Brunswick. « UNB is Canada's cybersecurity research hub » : https://www.unb.ca/cic/about/hub.html

Efforts de développement de la main-d'œuvre en cybersécurité au Nouveau Brunswick : Au-delà de la formation universitaire formelle

Développement de la main-d'œuvre : En dehors des entreprises

Le développement d'une main-d'œuvre solide et durable dépend de l'effort collectif du milieu de l'éducation, du gouvernement et de l'industrie privée. Plus de 70 % des répondants aux entrevues ont expressément mentionné les efforts fructueux de développement de la main-d'œuvre de CyberNB, l'association d'industries sans but lucratif de la province. Précisément, 40 % de ces répondants ont parlé de l'engagement du CyberNB à l'égard du programme éducatif CyberTitan pour les élèves de la maternelle à la 12e année. CyberTitan, une initiative du CTIC, est un concours éducatif en ligne conçu pour préparer au marché du travail les élèves possédant des compétences en cybersécurité très recherchées par les recruteurs de l'industrie[70]. De plus, deux répondants ont mentionné l'Initiative conjointe de développement économique, un programme de formation en cybersécurité conçu pour promouvoir le bassin d'Autochtones du Nouveau-Brunswick, remédier aux pénuries de main-d'œuvre et utiliser une approche d'apprentissage intégrée pour créer des bassins de main-d'œuvre inclusifs.

L'industrie privée est l'un des principaux bienfaiteurs des investissements en cybersécurité de la maternelle à la 12e année et au niveau postsecondaire. La grande majorité (environ 80 %) des personnes interrogées dans le secteur privé affirmaient participer à des programmes éducatifs, que ce soit par le biais de projets de sensibilisation dans l'industrie, de formations, de comités consultatifs de programme à l'échelle collégiale ou de programmes de mentorat. Plus de la moitié de ces répondants ont mentionné qu'ils avaient personnellement fait du bénévolat, en dehors du travail, pour contribuer à des projets de développement de la main-d'œuvre. Ces activités incluent des programmes de sensibilisation auprès des éducateurs et des étudiants (p. ex. discussions en classe, séminaires, activités parascolaires), du mentorat individuel, des événements de réseautage dans l'industrie, des projets en STIM (sciences, technologie, ingénierie et mathématiques) pour les filles, des conférences auprès d'étudiants et dans l'industrie, ainsi que des projets visant les groupes sous-représentés.

Perfectionnement professionnel ou formation à l'interne

Alors que le besoin de compétences spécialisées continue d'augmenter dans une profession en cybersécurité qui prend de l'ampleur, le personnel d'une organisation doit demeurer tout aussi dynamique. Des employés qui ont reçu une formation d'analystes des vulnérabilités pourraient maintenant devoir assumer des tâches d'architectes de systèmes de sécurité, exigeant des compétences supplémentaires qu'ils ne possédaient peut-être pas à l'origine. Par conséquent, bon nombre d'organisations peuvent choisir de former leur propre personnel au sein de nouvelles disciplines plutôt que de sonder le bassin de talents du Nouveau-Brunswick.

[70]*Pour de plus amples renseignements, consultez le site https://www.cybertitan.ca/*

Un des répondants de l'industrie a expliqué que le besoin croissant de son organisation pour des compétences spécialisées rendait le processus d'embauche trop complexe. Son organisation a choisi de concevoir des programmes de formation interne spécialisés à l'intention du personnel de divers degrés de complexité et de difficulté. Dans l'ensemble, environ la moitié des personnes interrogées ont confirmé qu'elles avaient investi dans la formation et le perfectionnement professionnel pour retenir en poste les talents qualifiés. Les autres commentaires intéressants formulés par les chefs de file de l'industrie concernant la formation et le perfectionnement professionnel incluent les suivants :

- Les organisations encouragent les programmes de mentorat interne afin de permettre aux nouveaux employés d'apprendre de spécialistes chevronnés de l'industrie;
- Les diplômés universitaires et collégiaux se voient souvent offrir des possibilités d'apprentissage intégré au travail s'ils leur manquent des qualifications ou une expertise précise[71];
- Il est important de fournir une formation spécialisée en matière juridique, politique et stratégique aux membres du personnel afin de les aider à mieux comprendre la réglementation et la gouvernance du gouvernement fédéral et à l'échelle internationale;
- L'encouragement de l'éducation autodirigée, aidée de subventions financières, pour des certifications de formation et la formation de travailleurs (certifications SANS, coûts de la certification CISSP, certification de piratage éthique) s'est révélé prometteur.

[71] *Comme https://www.wil-ait.digital/fr/*

Possibilités :

REMÉDIER À LA PÉNURIE DE MAIN D'ŒUVRE EN CYBERSÉCURITÉ

Le bassin de main-d'œuvre en cybersécurité au Nouveau-Brunswick est solide : il comprend des placements professionnels découlant de plusieurs programmes collégiaux et universitaires, ainsi que diverses possibilités de perfectionnement pour les professionnels formés en TI qui désirent se tourner vers une spécialisation en cybersécurité. Malgré ces possibilités, il n'existe que peu de données probantes indiquant que ces possibilités ont influencé positivement le marché du travail au cours des quatre dernières années. Comme le montre la figure 1, l'emploi au sein des professions en cybersécurité de la CNP dans la province est inférieur à ce qu'il était il y a cinq ans. En effet, diverses autres sources de données qui explorent de plus près les rôles en cybersécurité montrent toutes une tendance à l'égard de la demande de talents qualifiés, c'est-à-dire une demande pour des emplois qui requièrent plus d'années d'expérience minimale. De plus, les employeurs, autant ceux interrogés dans le sondage du CTIC que lors des entrevues, insistent constamment sur la nécessité d'embaucher des talents ayant déjà une expérience de l'industrie. Par conséquent, il est clair que la demande est forte, mais pas systématiquement : elle varie selon le rôle, et les nouveaux diplômés ne pourront pas nécessairement terminer leur programme et répondre immédiatement aux besoins des employeurs. Aussi, certains efforts de perfectionnement de la main-d'œuvre pourraient malencontreusement viser à soutenir un bassin de candidats de premier échelon dans des secteurs à faible croissance.

Les répondants de l'industrie soutenaient cet exposé des faits voulant que le bassin de talents ne réponde pas aux besoins de l'industrie, faisant remarquer que malgré le grand nombre de candidats, peu d'entre eux possédaient l'expérience pratique stable découlant notamment des programmes d'enseignement coopératif ou des possibilités d'apprentissage intégré au travail. Les personnes interrogées ont précisé qu'il était très difficile de trouver des candidats possédant des compétences précises puisque le domaine se diversifie de plus en plus en offrant divers rôles et sous-secteurs. Il devient de plus en plus difficile pour les programmes généralistes de premier échelon d'offrir aux étudiants un niveau satisfaisant d'exposition à l'industrie.

Par conséquent, quelles sont les possibilités de former des talents en cybersécurité hautement qualifiés au Nouveau-Brunswick?

Différentes recommandations se sont dégagées des entrevues et des données secondaires.

Améliorer le perfectionnement professionnel et la formation en cybersécurité des professionnels existants. La majorité des employeurs internationaux (57 %) ont indiqué qu'ils mettaient l'accent sur la formation du personnel comme moyen d'améliorer leur rendement en matière de cybersécurité[72]. De plus, les efforts de perfectionnement de la main-d'œuvre en cybersécurité du Nouveau-Brunswick semblent davantage cibler la formation de premier échelon que le perfectionnement des travailleurs actuels qui pourraient avoir besoin d'une expérience ou de compétences supplémentaires pour obtenir des postes de niveau supérieur.

Identifier des professionnels à mi-carrière qui possèdent une formation pertinente et des compétences transférables. Par exemple, Anciens Combattants Canada estime que plus de 30 000 personnes qualifiées habitent au Nouveau-Brunswick, dont 25 000 sont probablement bien en âge de travailler[73].

[72] *ISACA. State of cybersecurity 2019: Current trends in workforce development, 2019, p. 12.*
[73] *https://www.veterans.gc.ca/fra/about-vac/news-media/facts-figures/1-0*

Leur expérience de collaboration, selon des délais stricts et sous forte pression, s'inscrit dans la portée des besoins de main-d'œuvre qualifiée en cybersécurité. Aux États-Unis, les entreprises technologiques ont commencé à établir des bassins de recrutement direct dans l'armée pour doter les emplois spécialisés, réalisant que le nombre de nouveaux diplômés ne concorde pas avec le besoin croissant de candidats de qualité[74].

Officialiser des parcours professionnels bien définis en cybersécurité que les nouveaux diplômés peuvent suivre pour acquérir l'expérience et les compétences nécessaires, comprendre les possibilités d'avancement et planifier leur carrière. Plutôt que de chercher des professionnels en cybersécurité qui connaissent bien tous les domaines, la définition d'ensembles de compétences compartimentées et de parcours professionnels clairs améliorera la formation et clarifiera les compétences clés que doivent posséder les recrues lorsqu'elles arrivent sur le marché du travail[75]. Plus précisément, dans la province du Nouveau-Brunswick, il pourrait s'agir d'accroître le nombre de possibilités d'apprentissage intégré au travail ou d'enseignement coopératif offertes et leur durée. Cette mesure est particulièrement importante étant donné la main-d'œuvre vieillissante dans la province.

Traiter de la sous-représentation et des possibilités d'avancement inégales des professionnels en cybersécurité qui s'identifient comme des femmes et des minorités[76]. La question de la sous représentation des femmes a été difficile à ébranler dans l'histoire de l'industrie de la cybersécurité, et en Amérique du Nord, le nombre de programmes de diversité organisationnelle (la plupart ayant souvent une orientation de genre) diminue probablement année après année, suivant une tendance à la baisse en plus des perceptions des employeurs quant à leur efficacité[77]. Toutefois, la hausse du nombre de jeunes femmes détenant un diplôme en TIC pourrait aider les employeurs à recruter activement davantage de femmes en cybersécurité, à les payer équitablement, et à leur offrir les mêmes possibilités d'avancement que leurs homologues masculins[78]. Comme discuté précédemment, une meilleure diversité et l'égalité des chances dans le secteur de la cybersécurité élargiraient le bassin de recrues potentielles.

Mener une analyse plus poussée des parcours professionnels clairs pour les recrues internationales. Comme l'indique la section sur les nouveaux arrivants et les immigrants, plusieurs des employeurs interrogés ont parlé des difficultés qu'ils ont rencontrées et des longues périodes d'attente en lien avec les processus d'immigration pour plusieurs raisons, dont certaines concernent les autorisations de sécurité et le travail avec des partenaires internationaux comme les États-Unis. Une analyse plus approfondie de ce qui peut être fait pour améliorer l'expérience des nouveaux arrivants, des efforts de promotion des associations provinciales et des défis auxquels font face les employeurs en cybersécurité pendant le processus de recrutement est nécessaire. Certains changements stratégiques clés dans ce domaine pourraient radicalement améliorer le bassin de talents qualifiés à mi-carrière.

[74]https://www.itprotoday.com/strategy/it-reaps-benefits-military-veteran-hiring-programs
[75]Deloitte and Toronto Financial Services Alliance. The changing faces of cybersecurity: Closing the cyber risk gap, 2018.
[76]Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, p. 6.
[77]ISACA. State of cybersecurity 2019: Current trends in workforce development, 2019, p. 16.
[78]Center for Cyber Safety and Education. The 2017 Global Information Security Workforce Study: Women in Cybersecurity, Frost & Sullivan. 2017.

Accroître la loyauté des jeunes travailleurs, qui sont plus susceptibles de quitter leur emploi et d'exprimer leur insatisfaction à l'égard des rôles existants[79], en offrant une formation en milieu de travail, une diversité de rôles, le paiement des certifications par l'employeur, et du soutien pour le télétravail ou le travail flexible, entres autres considérations[80]. Alors que le maintien en poste des jeunes travailleurs représente un défi au Nouveau-Brunswick, la création de meilleurs parcours professionnels et de perspectives encouragera ce groupe démographique à demeurer dans sa province d'origine tout en attirant de nouveaux venus.

Utiliser les nouvelles technologies pour accroître la sécurité et réduire les risques[81]. Dans l'ensemble, 18 % des organisations interrogées membres de l'ISACA ont indiqué qu'elles commençaient à faire de plus en plus appel à l'intelligence artificielle pour réduire les lacunes de l'organisation en matière de cybersécurité[82]. Ce thème a été partagé par les intervenants interrogés et représente un complément majeur aux efforts de perfectionnement de la main-d'œuvre, mais ne constitue pas le but premier de la présente étude.

[79]Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, p. 6.
[80]Center for Cyber Safety and Education (ISC)2. « Meet the Millennials », Frost & Sullivan, 2017 : https://iamcybersafe.org/MeetTheMillennials.
[81]Deloitte and Toronto Financial Services Alliance. The changing faces of cybersecurity: Closing the cyber risk gap, 2018, p. 6.
[82]ISACA. State of cybersecurity 2019: Current trends in workforce development, 2019, p. 12.

Conclusion

Dans le domaine en rapide évolution de la cybersécurité, la province du Nouveau-Brunswick offre une perspective unique en tant que petit écosystème bien réseauté doté d'organisations spécialisées qui jouent un rôle concret dans le perfectionnement de la main-d'œuvre. La province profite d'avantages relatifs, notamment des investissements du secteur public, de grands joueurs de l'industrie et une grande qualité de vie, mais doit aussi composer avec certains désavantages, comme son éloignement et son taux de chômage élevé. Cependant, globalement, la province réussit à bien tirer son épingle du jeu, notamment en ce qui concerne les emplois, à l'égard de la population, du perfectionnement de la main d'œuvre et des établissements d'enseignement. Les rôles recherchés au Nouveau-Brunswick incluent bon nombre d'emplois très spécialisés qui sont généralement occupés par une main-d'œuvre expérimentée, mais vieillissante, et toutes les données probantes suggèrent que ces travailleurs qualifiés plus âgés sont plus difficiles à trouver et à retenir que les candidats de premier échelon. En plus de certaines possibilités démographiques, les importants efforts de perfectionnement de la main d'œuvre déployés par la province sont suffisamment pertinents pour relever les défis recensés dans le présent rapport, créant des parcours professionnels solides et clairs pour retenir les jeunes arrivants sur le marché du travail, envisageant des façons d'uniformiser les processus de recrutement et d'immigration pour les talents internationaux, ainsi que retenir et perfectionner les professionnels existants.

Annexe

I Méthodes et outils de recherche

La présente étude comprenait un examen exhaustif de la littérature pertinente et une analyse des données secondaires, l'utilisation de données recueillies sur le Web, ainsi que deux principaux outils de recherche primaire, décrits ci-dessous.

Examen de la littérature secondaire, des données et des données recueillies sur le Web

Un examen initial de la littérature portait sur les études s'appliquant au perfectionnement de la main d'œuvre en cybersécurité et les besoins en main-d'œuvre au Canada, aux États-Unis et ailleurs dans le monde, et un examen secondaire de la littérature visait les parcours professionnels et les options d'éducation en cybersécurité au Nouveau-Brunswick. L'examen des données secondaires ciblait l'information existante sur la demande en cybersécurité, provenant principalement de Statistique Canada. De plus, un moissonnage du Web exhaustif a été effectué pour recueillir des informations sur le nombre d'avis d'emplois en cybersécurité au Nouveau-Brunswick affichés d'août 2019 à janvier 2020, les comparant aux données canadiennes. Une liste exhaustive des termes de recherche sur le Web (titres d'emplois, compétences et certifications en cybersécurité) a été générée par le **comité consultatif** de l'étude, un groupe ayant de l'expertise dans le domaine qui a fait un suivi des progrès des recherches dans le cadre de trois rencontres du comité consultatif : une rencontre de lancement en juillet 2019, une rencontre intérimaire en novembre 2019, et une rencontre de validation en février 2020.

Professions en TIC – Liste des codes de la CNP

rvey, distributed by ICTC in autumn 2019, was shared with a purposive sample of 178 organiza-
Dans le cadre de cette étude, lorsque des taux de chômage sont présentés pour le secteur des TIC au Canada ou au Nouveau-Brunswick, les chiffres incluent les codes de la CNP suivants.

Code CNP	Description
0015	Cadres supérieurs – commerce, radiotélédiffusion et autres services, n.c.a.
0211	Directeurs des services de génie
0213	Gestionnaires des systèmes informatiques
0601	Directeurs des ventes corporatives
1123	Professionnels en publicité, en marketing et en relations publiques

1253	Techniciens à la gestion des documents
2133	Ingénieurs électriciens et électroniciens
2147	Ingénieurs informaticiens (sauf les ingénieurs et les concepteurs en logiciels)
2148	Autres ingénieurs, n.c.a.
2161	Mathématiciens, statisticiens et actuaires
2171	Consultants et analystes des systèmes d'information
2172	Analystes de bases de données et administrateurs de données
2173	Ingénieurs et concepteurs en logiciels
2174	Programmeurs informatiques et développeurs de médias interactifs
2175	Développeurs et concepteurs Web
2241	Techniciens et technologues en génie électrique et électronique
2281	Techniciens de réseau informatique
2282	Techniciens de soutien aux utilisateurs
2283	Techniciens en essai de systèmes
4163	Agents de développement économique, recherchistes et experts-conseils en marketing
5223	Techniciens en graphisme
5224	Techniciens en radiotélédiffusion
5241	Concepteurs et illustrateurs graphiques
7241	Électriciens (sauf électriciens industriels et de réseaux électriques)
7242	Électriciens industriels
7243	Électriciens de réseaux électriques
7244	Monteurs de lignes électriques et de câbles
7245	Monteurs de lignes et de câbles de télécommunications
7246	Installateurs et réparateurs de matériel de télécommunications
7247	Techniciens en montage et en entretien d'installations de câblodistribution

Outils de recherche primaire

Sondage auprès des employeurs en cybersécurité du Nouveau-Brunswick. Ce sondage, mené par le CTIC à l'automne 2019, a été partagé avec un échantillon choisi à dessein de 178 organisations identifiées comme (a) étant basées au Nouveau-Brunswick ou y ayant une présence physique, et (b) embauchant du personnel en cybersécurité, dans une variété de secteurs et d'industries. Les répondants cibles étaient des cadres supérieurs familiers avec les besoins d'embauche en cybersécurité dans la province. Les organisations étaient encouragées à partager et à redistribuer le sondage, le cas échéant.

Au total, le sondage comptait 54 réponses, dont 8 ont été éliminées en raison de la mauvaise qualité des données. Des 46 réponses restantes, 41 ont été validées comme étant complètes et pertinentes, alors que les 5 autres étaient seulement partiellement complètes. Elles provenaient toutefois d'organisations pertinentes et, à ce titre, ont été étudiées pour certaines parties de l'analyse (pour un taux de réponse de 23 à 26 %, pour 41 réponses complètes à 46 réponses partielles, respectivement). Le sondage posait des questions au sujet de l'organisation, de sa main-d'œuvre actuelle en cybersécurité, de ses besoins en main-d'œuvre, et de ses priorités en matière d'emploi et de compétences.

Entrevues auprès d'intervenants clés. L'étude comprenait 16 entrevues auprès de professionnels supérieurs en cybersécurité travaillant au Nouveau-Brunswick. Ces entrevues approfondies semi structurées ont été menées auprès de professionnels ayant une expertise de l'industrie ou des politiques pertinentes dans la région ciblée. Deux répondants représentaient la même organisation, et tous les autres provenaient d'entreprises différentes. Les entrevues duraient de 45 minutes à 1 heure, et un aperçu détaillé des protocoles de confidentialité et des paramètres de l'étude a été présenté aux répondants avant le début des entrevues. Les questions portaient sur les analyses de rentabilisation des organisations, la main-d'œuvre actuelle et idéale en cybersécurité, les efforts de recrutement et les efforts de perfectionnement de la main-d'œuvre. Les conversations ont également exploré l'écosystème de cybersécurité de la province du Nouveau-Brunswick, les relations entre les secteurs public et privé, et les possibilités économiques uniques dans le domaine au sein de la province.

Limites et possibilités de recherches futures

Certaines limites ont été soulevées au cours de l'étude. En ce qui concerne la littérature et les données secondaires, certaines analyses se fondent sur des informations provenant de Statistique Canada qui sont éliminées en deçà d'un certain seul[83] afin de protéger l'anonymat des participants : cette mesure s'applique surtout aux données de l'Enquête sur la population active pour le Nouveau-Brunswick. Pour les données de l'Enquête sur la population active, les mois supprimés ont été éliminés de l'ensemble de données afin d'écarter les chiffres artificiellement faibles. De plus, cette étude repose largement sur l'Enquête canadienne sur la cybersécurité et le cybercrime de Statistique Canada (2017), laquelle ne propose que des chiffres à l'échelle nationale. Lors des consultations avec l'équipe de recherche, Statistique Canada a indiqué que cette enquête nationale n'était pas conçue pour établir des ventilations régionales, en partie en raison du caractère sans frontière de la cybercriminalité : à ce titre, il est difficile de recueillir des perspectives propres au Nouveau-Brunswick à partir de cette source en particulier.

Le processus de moissonnage du Web du CTIC a été mené sur une période de six mois, soit d'août 2019 à janvier 2020. Lors des futures recherches, il serait intéressant d'évaluer le nombre d'emplois affichés au printemps et en été. L'analyse des données recueillies sur le Web a permis d'établir plusieurs hypothèses, soit (a) qu'un avis affiché équivalait à un emploi, et (b) que l'affichage des mêmes titres d'emploi, description et entreprise pendant plus d'un mois signifiait qu'un poste n'était pas doté, et non pas que l'avis avait été republié.

[83]Le seuil varie selon la province et est établi à 500 personnes ou emplois pour le Nouveau-Brunswick. Pour de plus amples renseignements, consultez le site https://www23.statcan.gc.ca/imdb/p2SV_f.pl?Function=getSurvey&SDDS=3701

De plus, comme l'indique l'étude, les emplois ne sont pas tous affichés : par conséquent, il est possible que cet ensemble de données ne tienne pas compte de certains rôles en cybersécurité offerts dans la province.

En ce qui concerne la collecte de données primaires, le sondage auprès des employeurs a enregistré un taux de réponse qui correspondait à l'échelle normalisée pour la distribution de courriels externes (de 23 à 26 % pour les réponses complètes et valides, respectivement, voir ci-dessus), mais les futures recherches devraient tenter d'étudier un échantillon d'au moins 100 employeurs ayant de l'expertise de l'embauche en cybersécurité au Nouveau-Brunswick pour guider des conclusions supplémentaires.

Le comité consultatif du projet a cerné plusieurs secteurs potentiels de futures recherches constructives.

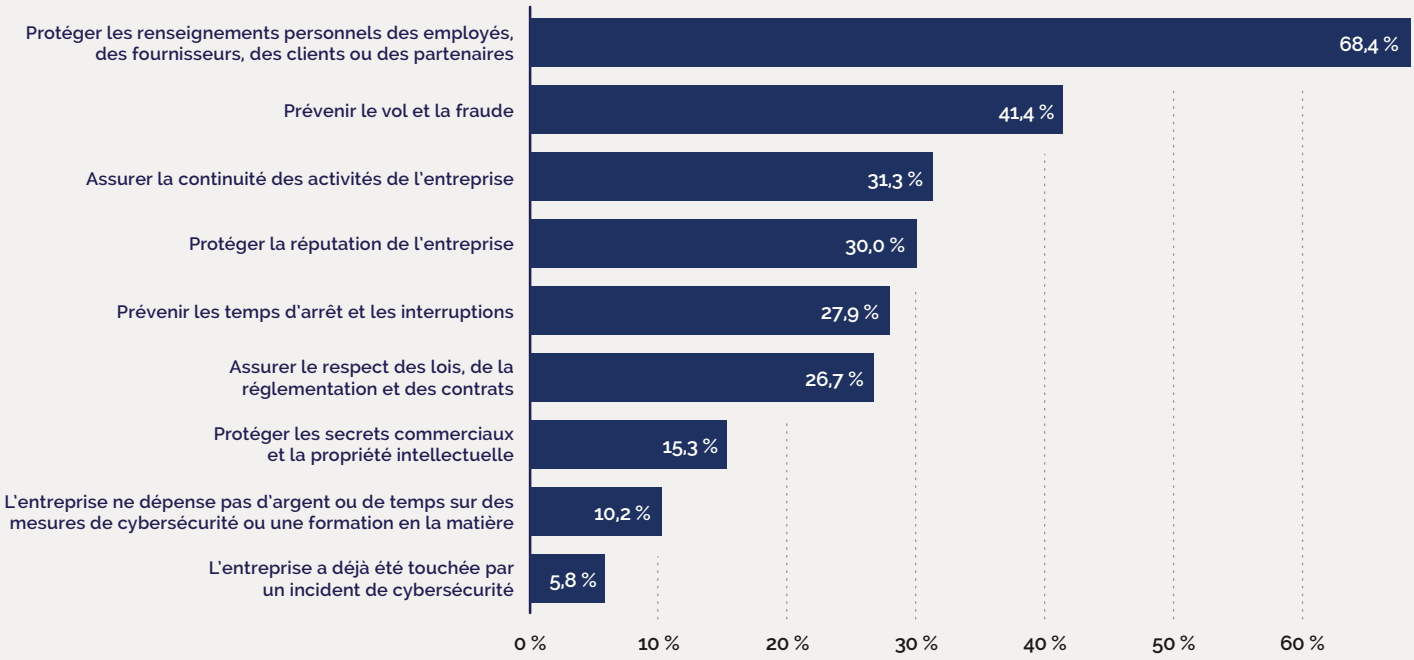
- Bien que la collecte de données exhaustives sur la sous-traitance ne faisait pas partie de la portée de la présente étude, il serait utile pour les membres de l'industrie et les chercheurs d'emploi au Canada que des recherches soient réalisées sur les types d'emplois en cybersécurité qui sont externalisés, dans quels pays et pourquoi.
- Le nombre de femmes en cybersécurité est demeuré faible pendant de nombreuses années : il serait intéressant de mener une étude panprovinciale pour déterminer quels domaines des sciences attirent les femmes, et ne les attirent pas, et pourquoi.
- Dans le cadre des entrevues, cette étude a exploré les obstacles à l'embauche de talents qualifiés, et la question des protocoles de sécurité et des critères de sélection stricts et problématiques pour les immigrants était un thème récurrent. Les futures recherches pourraient explorer des moyens efficaces de revisiter les processus actuels afin d'identifier et d'intégrer les nouveaux venus à la main-d'œuvre canadienne.
- Il serait intéressant de savoir, en détail, d'où proviennent les étudiants collégiaux et universitaires en cybersécurité (lieu et formation académique) et où ils sont embauchés. En d'autres termes, bien que cette étude se voulait surtout une analyse de la demande de la main d'œuvre en cybersécurité, les futures recherches devraient chercher à explorer en profondeur l'offre et la demande, analysant la formation, le processus d'immigration et les parcours professionnels afin de mieux comprendre le portrait complet de la main-d'œuvre en cybersécurité au Nouveau-Brunswick.

II Autres chiffres

Dans la section La demande en cybersécurité : Employeurs par secteur et taille, la présente étude explore les raisons pour lesquelles les entreprises du secteur privé du Canada *ne disposent pas* de personnel en cybersécurité. Cependant, ce même sondage propose des données sur les raisons pour lesquelles les entreprises *embauchent* du personnel dédié à la cybersécurité, comme l'indique la figure ci-après.

Raisons de prioriser la cybersécurité : Moyenne dans le secteur privé

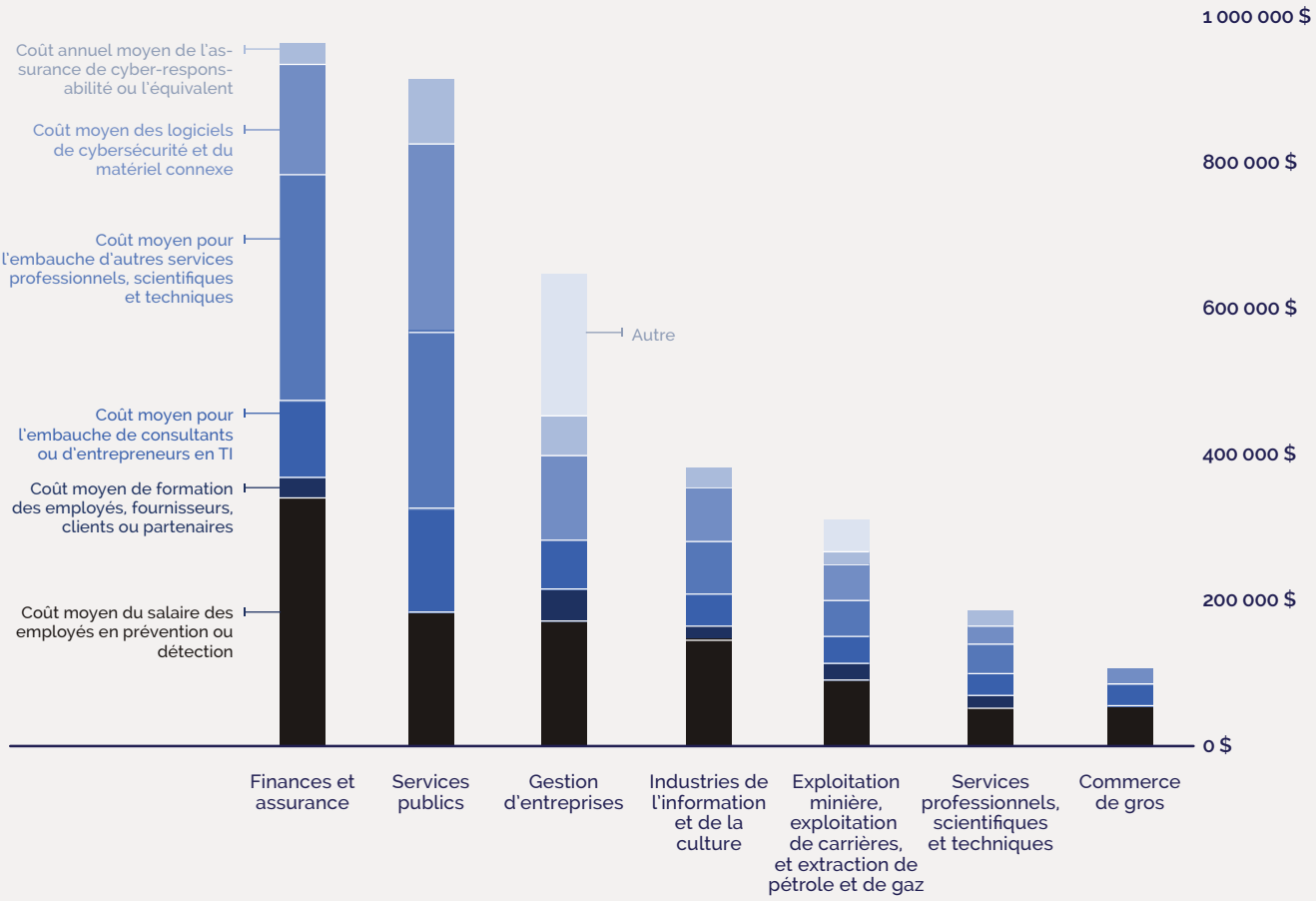
Principales raisons de prioriser la cybersécurité, par % de répondants qui ont choisi chacune des réponses



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime 2017

Aussi, l'Enquête canadienne sur la cybersécurité et le cybercrime (2017) de Statistique Canada examine les secteurs qui dépensent le plus d'argent en cybersécurité, et les fins auxquelles cet argent est utilisé. Il est évident que l'embauche et les salaires représentent la principale dépense, les logiciels de cybersécurité arrivant au deuxième rang (bien que les coûts varient grandement selon l'industrie).

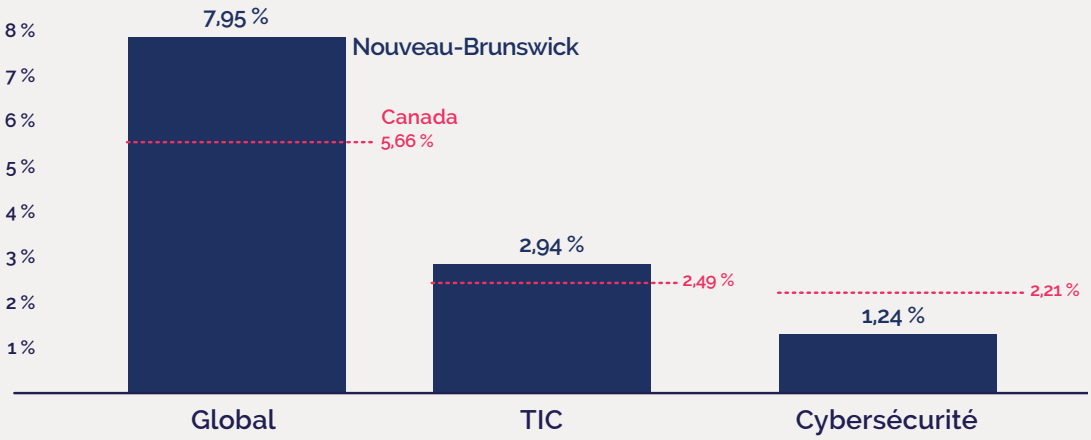
Industries qui investissent dans la cybersécurité par rapport à la moyenne dans le secteur privé



Source : Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime 2017

Bien que la figure 1 de l'étude illustre le taux de chômage au fil du temps, le chiffre ci-dessous propose une comparaison entre trois différents taux de chômage pour le Canada et le Nouveau-Brunswick en 2019, utilisant les mêmes définitions de la CNP de ces secteurs comme décrites dans le texte.

Taux de chômage par région, 2019



Source : Enquête sur la population active de Statistique Canada