Deloitte.

TFSA | TORONTO FINANCIAL SERVICES ALLIANCE

Les différents visages de la cybersécurité

Combler les lacunes liées aux cyberrisques

Cyberrisque

Table des matières

Sommaire

Le monde fait face à une pénurie chronique de talents en cybersécurité. En effet, l'évolution constante des nouvelles technologies et des cybermenaces donne lieu à une telle augmentation des cyberrisques que les équipes de cybersécurité existantes peinent à suivre le rythme.

Dans ce rapport, nous présentons une nouvelle façon de considérer les talents en cybersécurité, en utilisant un cadre centré sur l'aspect humain qui nous permet d'examiner le défi du Canada relatif aux cybertalents, l'évolution de la situation ainsi que les principaux moyens à la disposition des entreprises, des établissements d'enseignement et des gouvernements pour surmonter la pénurie de talents et combler les lacunes liées aux cyberrisques.

Nos constatations et notre analyse sont fondées sur des discussions et des entretiens réalisés avec plus de 40 leaders, enseignants et administrateurs canadiens du domaine de la cybersécurité, ainsi que sur un sondage approfondi mené auprès de plus de 110 dirigeants canadiens du secteur des services financiers et d'autres secteurs clés de notre économie.

Défi du Canada relatif aux cybertalents

Les organisations de partout au pays sont touchées par l'évolution technologique et la nécessité d'améliorer constamment leurs capacités sur le plan de la cybersécurité. Cette tendance a entraîné une demande sans précédent de professionnels de la cybersécurité, faisant de la pénurie de cybertalents l'un des défis les plus importants du Canada.

Deloitte et la Toronto Financial Services Alliance se sont associés pour comprendre le problème et proposer une solution. Ce que l'on a constaté : les défis et les possibilités sont semblables partout au pays, que vous soyez un chef de file dans le secteur des services financiers, du commerce de détail ou de l'énergie et des ressources.

Selon notre analyse, la demande en cybertalents au Canada augmente de 7 % par année, ce qui signifie que les organisations devront pourvoir environ 8 000 postes de professionnels de la cybersécurité entre 2016 et 2021. Les entreprises, les gouvernements et les universités prennent toutes les mesures nécessaires pour pallier la pénurie de cybertalents. Toutefois, leurs efforts et leurs approches ne suffiront probablement pas pour résoudre le problème.

Les différents visages de la cybersécurité

Pour combler toutes les lacunes, il faudra mener une nouvelle réflexion et adopter une nouvelle perspective ou, plus précisément, un nouveau cadre sur les cybertalents qui propose des façons nouvelles et novatrices de surmonter la pénurie de talents en considérant cette dernière sous un angle humain.

Le cadre de Deloitte sur les cybertalents s'axe sur sept personnalités de la cybersécurité – le stratège, le conseiller, le défenseur, le pompier, le bidouilleur, le scientifique et le détective. Ces personnalités mettent un visage humain sur les ensembles complexes de capacités requises pour assurer une cybersécurité efficace. Cette nomenclature aide les non-technologues à mieux comprendre ces capacités et permet de les définir de manière plus stable que le sont les descriptions et les exigences traditionnelles des cybertalents, qui tendent à mettre l'accent sur des compétences techniques très précises pouvant rapidement devenir obsolètes.

Il est particulièrement important que le cadre puisse demeurer pertinent et valide dans un contexte changeant, étant donné la rapidité à laquelle le secteur de la cybersécurité évolue.

Recommandations et prochaines étapes

Le fait de considérer l'écosystème canadien des cybertalents sous un angle humain permet de révéler des mesures essentielles à prendre qui touchent toutes les étapes du cycle de vie des employés, de la croissance du bassin de talents mondial au recrutement des bonnes personnes en passant par l'orientation des nouveaux employés, l'acquisition continue de nouvelles compétences et expertises, la fidélisation des meilleurs talents et même l'adoption d'une expérience de départ qui protège l'image de marque d'une organisation en matière de talents.

Les technologies émergentes telles que l'automatisation et l'intelligence artificielle peuvent et doivent être utilisées pour consolider les efforts déployés par une organisation en matière de cybersécurité. Cependant, ces technologies n'éliminent pas la nécessité d'avoir recours à des experts humains.

Les gouvernements de tous les paliers jouent un rôle important dans l'écosystème des talents en cybersécurité, non seulement parce qu'ils doivent retenir les services de ces talents pour protéger les données et les systèmes publics, mais aussi parce qu'ils élaborent des politiques et des programmes pour remédier à la pénurie de talents.

1 Introduction

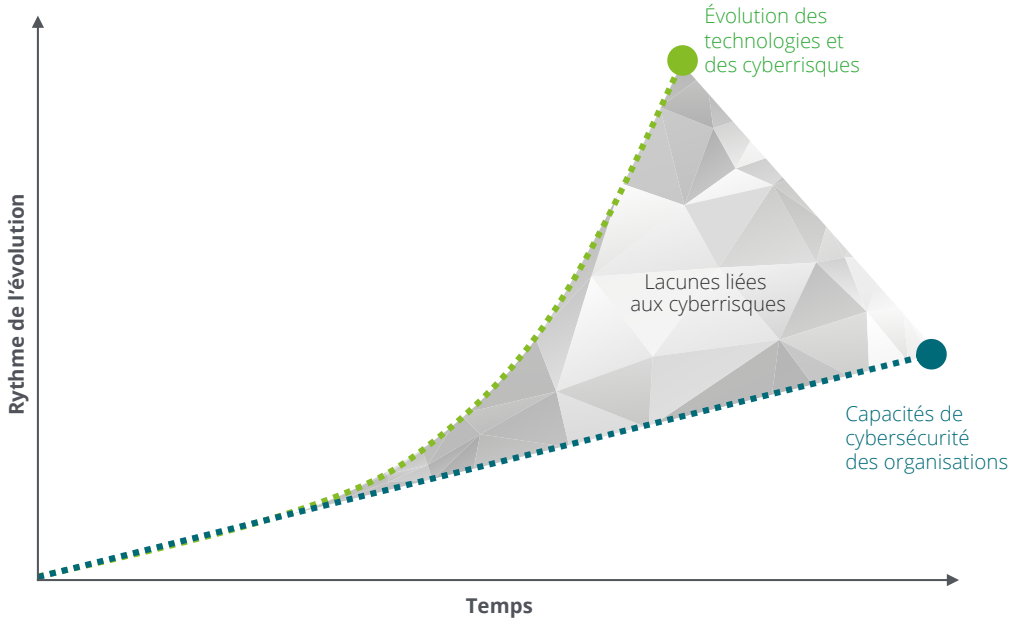
Les cyberrisques dans un monde automatisé, ouvert et axé sur les données

L'évolution rapide des technologies modifie la façon dont les entreprises exercent leurs activités. Les technologies émergentes telles que l'Internet des objets, l'infonuagique, l'automatisation et l'intelligence artificielle rendent possible l'adoption de nouveaux modèles d'affaires automatisés, ouverts et axés sur les données ainsi que la concrétisation d'un nombre sans précédent d'occasions de création de valeur.

Cette valeur n'est cependant pas garantie. À mesure que les technologies progressent, le degré de cyberrisque auquel les organisations doivent faire face augmente également. En fait, les analystes estiment que les cyberrisques à l'échelle mondiale « pourraient ralentir le rythme de l'innovation technologique en engendrant une perte économique évaluée à trois billions de dollars en 2020[1] ».

Malheureusement, l'évolution rapide des technologies et des cyberrisques connexes semble dépasser la capacité d'adaptation des organisations. Malgré des investissements importants en cybersécurité au cours de la dernière décennie, des organisations de tous les secteurs constatent des lacunes grandissantes en matière de cyberrisques. (Voir la figure 1.)

Figure 1 : Lacunes grandissantes liées aux cyberrisques



Les catalyseurs du cyberrisque :

- Prolifération des données personnelles en ligne et augmentation de leur valeur économique
- Surface de cyberattaque plus étendue
- Sophistication des cybermenaces
- Augmentation des pressions des consommateurs et de la réglementation en matière de sécurité et de confidentialité

Combler les lacunes liées aux cyberrisques : le facteur humain

Réduire l'écart lié aux cyberrisques et permettre aux organisations de tirer pleinement parti des nouvelles technologies représentent un défi majeur de notre époque. Un élément essentiel dans cette quête est le facteur humain : les professionnels de la cybersécurité qui travaillent tous les jours pour protéger les systèmes et les données.

Ce n'est pas un secret, à l'échelle mondiale, les organisations sont confrontées à une pénurie croissante de professionnels de la cybersécurité. Selon les dernières estimations et si la tendance se maintient, « les lacunes liées à main-d'œuvre en cybersécurité se chiffreront à 1,8 million de travailleurs d'ici 2022, une augmentation de 20 % par rapport à la prévision faite en 2015[2] ». Il s'agit d'une annonce stupéfiante qui aura une incidence importante sur les entreprises et les gouvernements.

La bonne nouvelle est qu'un grand nombre des technologies entraînant l'augmentation des cyberrisques peuvent également être utilisées pour améliorer la productivité et réduire le recours à des experts humains hautement qualifiés dans un contexte de pénurie en cybertalents.

Ce concept, qui fait de plus en plus l'objet de recherches, se nomme la ***sécurité augmentée***[3]. (Voir la figure 2.)

Figure 2 : Sécurité augmentée

Ces possibilités sont prometteuses. Et, compte tenu de la pénurie grandissante de talents, les organisations n'ont d'autre choix que d'en tenir compte.

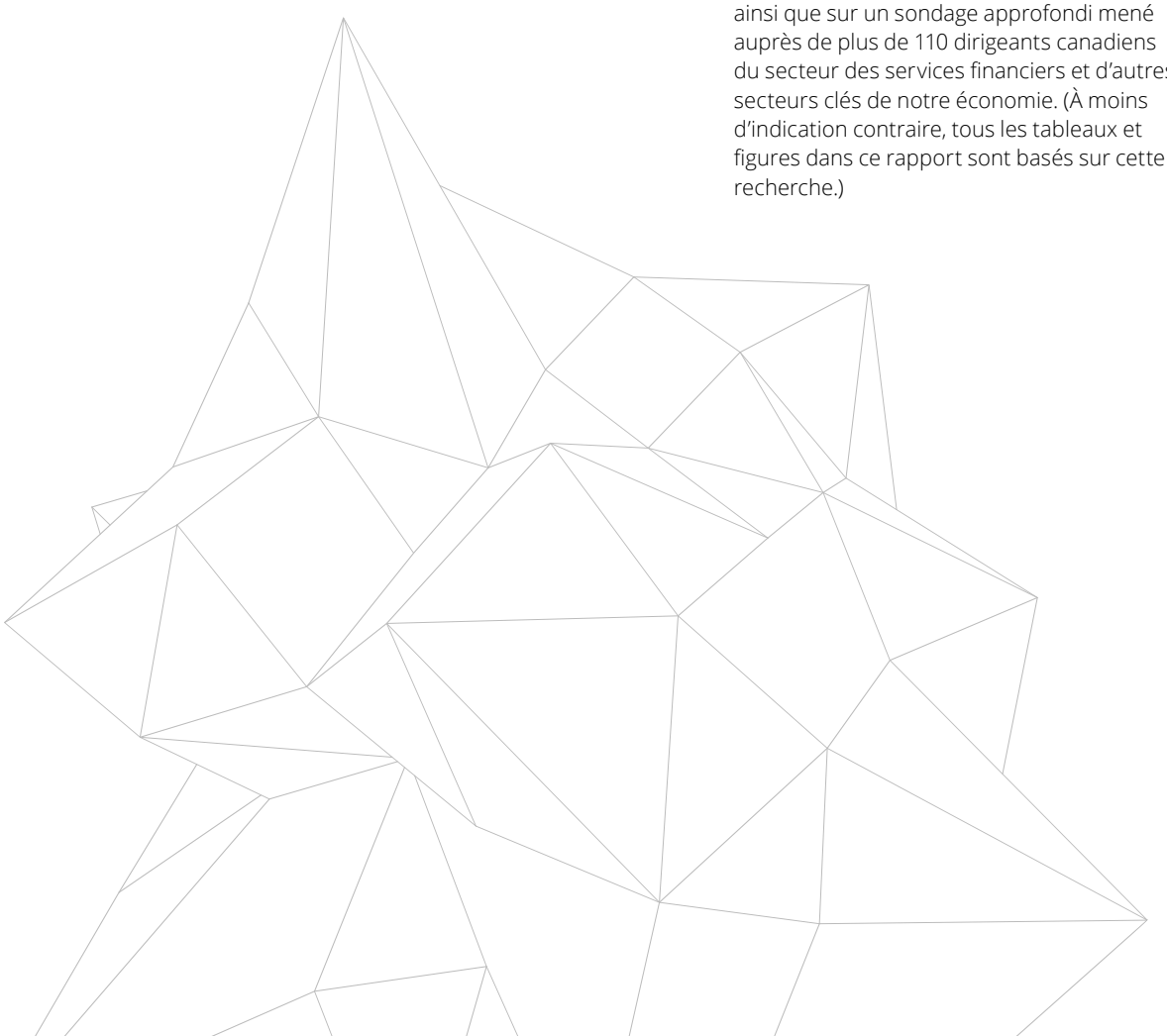
Cependant, même si les progrès technologiques vont générer une valeur notable pour les équipes de cybersécurité, la résolution de la pénurie de talents en cybersécurité nécessitera le déploiement d'efforts additionnels. En particulier, il faudra aborder le problème sous un angle différent et donner un visage humain aux défis et aux solutions.

Surmonter la pénurie de talents en cybersécurité

Cette étude, menée par Deloitte et la Toronto Financial Services Alliance, présente une nouvelle façon de considérer les talents en cybersécurité, en utilisant un cadre centré sur l'aspect humain qui nous permet de comprendre les différents visages de la cybersécurité.

Dans cette optique – en particulier au Canada –, nous examinons le défi auquel est confronté notre pays en ce qui concerne les talents en cybersécurité, l'évolution de la situation ainsi que les principaux moyens à la disposition des entreprises, des établissements d'enseignement et des gouvernements pour surmonter la pénurie de talents et combler les lacunes liées aux cyberrisques.

Cette recherche est fondée sur des discussions et des entretiens réalisés avec plus de 40 leaders, enseignants et administrateurs canadiens en cybersécurité, ainsi que sur un sondage approfondi mené auprès de plus de 110 dirigeants canadiens du secteur des services financiers et d'autres secteurs clés de notre économie. (À moins d'indication contraire, tous les tableaux et figures dans ce rapport sont basés sur cette recherche.)



2 Défi du Canada relatif aux cybertalents

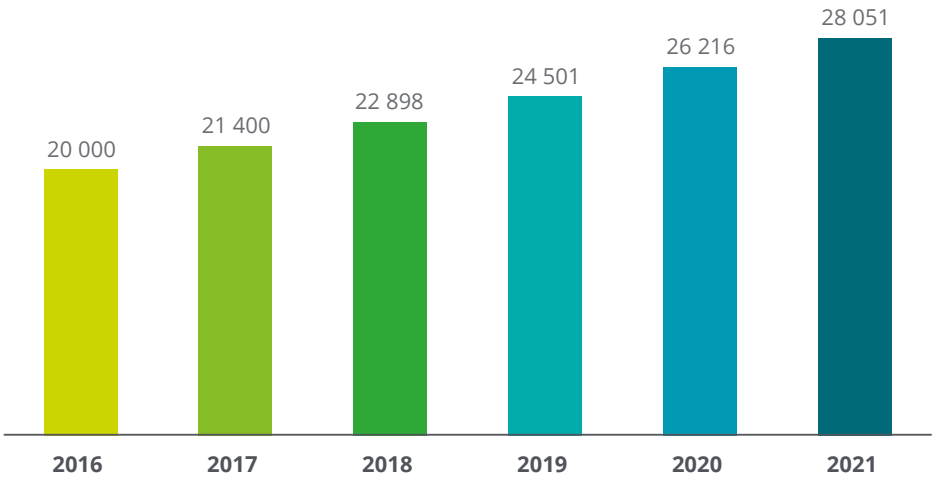
Tous les principaux secteurs du Canada – y compris les services financiers, le commerce de détail ainsi que l'énergie et les ressources – sont touchés par l'évolution technologique et doivent renforcer leurs capacités en matière de cybersécurité.

Cette tendance entraîne une augmentation de la demande de professionnels de la cybersécurité. Selon les données du Conseil des technologies de l'information et des communications (CTIC)[4] et de Statistique Canada[5], nous estimons que le Canada employait environ 20 000 professionnels de la cybersécurité, tous secteurs confondus, en 2016. Cette estimation prudente représente environ 1,6 % de tous les professionnels des technologies de l'information et de la communication (TIC) au pays.

À titre de référence, les analystes du secteur indiquent que les professionnels de la cybersécurité représentent généralement environ 5,9 % du personnel informatique d'une organisation. Si cette donnée est exacte, cela signifie que le problème est encore plus grave qu'on le croit.

D'ici 2021, nous estimons qu'il y aura environ 28 000 professionnels de la cybersécurité au Canada, ce qui représente un taux de croissance annuel d'environ 7 %; ils représenteraient alors près de 2 % de tous les professionnels des TIC. Si on extrapole ces données, cela suggère que les organisations canadiennes devront pourvoir quelque 8 000 postes dans le domaine de la cybersécurité entre 2016 et 2021. (Voir la figure 3.)

Figure 3 : Demande de cybertalents au Canada

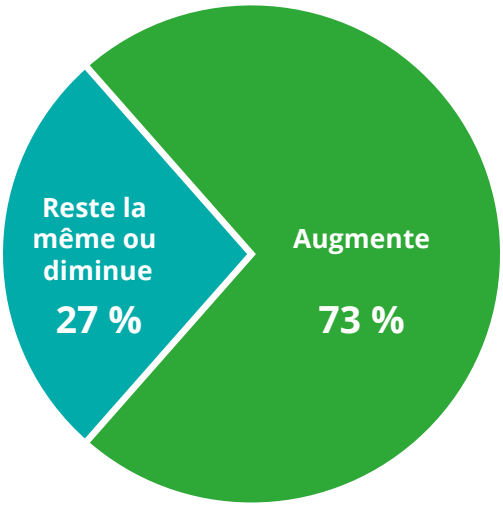


Source : Analyse de Deloitte fondée sur les données de ICTC, Statistique Canada, *Portrait de la scolarité au Canada : recensement de la population de 2016*, 2017, https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2017036-fra.htm

Ces estimations correspondent aux résultats de notre sondage. Selon le sondage, 73 % des dirigeants canadiens s'attendent à ce que le nombre d'employés à temps plein affectés à la cybersécurité augmente au cours des trois à cinq prochaines années; un quart des répondants s'attendent à une croissance de plus de 25 %. (Voir la figure 4.)

Comme ces statistiques l'indiquent, la demande de notre pays en professionnels de la cybersécurité devrait augmenter considérablement dans les années à venir. La question suivante se pose alors : Dans quelle mesure le Canada est-il prêt à relever ce défi en ce qui concerne les talents en cybersécurité, et comment les entreprises, les établissements d'enseignement et les gouvernements peuvent-ils surmonter ces obstacles?

Figure 4 : Tendances relatives à la croissance des talents en cybersécurité au sein des organisations



Entreprises

Les dirigeants canadiens considèrent la pénurie de talents en cybersécurité comme l'un des cinq principaux défis de la gestion de la cybersécurité au sein de leurs organisations. De plus, les quatre autres défis – l'évolution du contexte des menaces, le rythme des changements, les besoins de conformité liée à la sécurité et à la confidentialité ainsi que le caractère disparate des outils de sécurité – entraînent directement une hausse de la demande en cybertalents. (Voir la figure 5.)

Ces défis ne devraient pas s'atténuer de sitôt. Lorsqu'ils envisagent l'avenir, les répondants au sondage soulignent que l'augmentation de la fréquence et de la complexité des cybermenaces ainsi que la réglementation accrue relative à la sécurité et à la confidentialité seront les tendances les plus marquées sur le plan de la cybersécurité au cours des trois à cinq prochaines années.

Des entreprises canadiennes de premier plan prennent déjà des mesures pour pallier la pénurie de cybertalents. Cependant, en dépit de leurs efforts, trois défis précis continuent de se poser pour les responsables de la sécurité de l'information : la gestion du cycle de vie des talents, la productivité et l'inclusion.

Figure 5 : Principaux défis pour la gestion de la cybersécurité et des lacunes liées aux cyberrisques

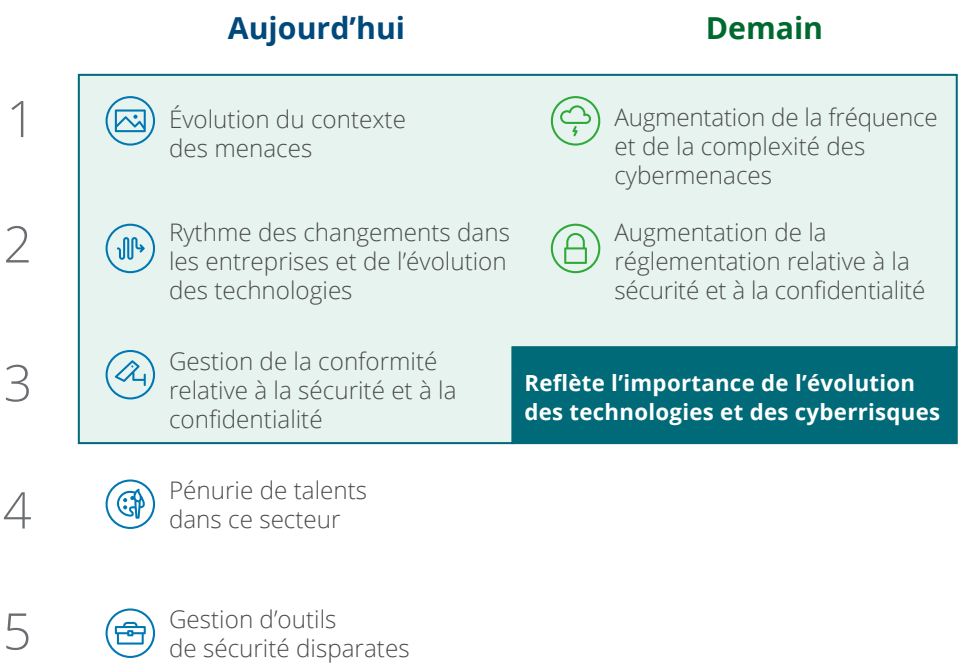
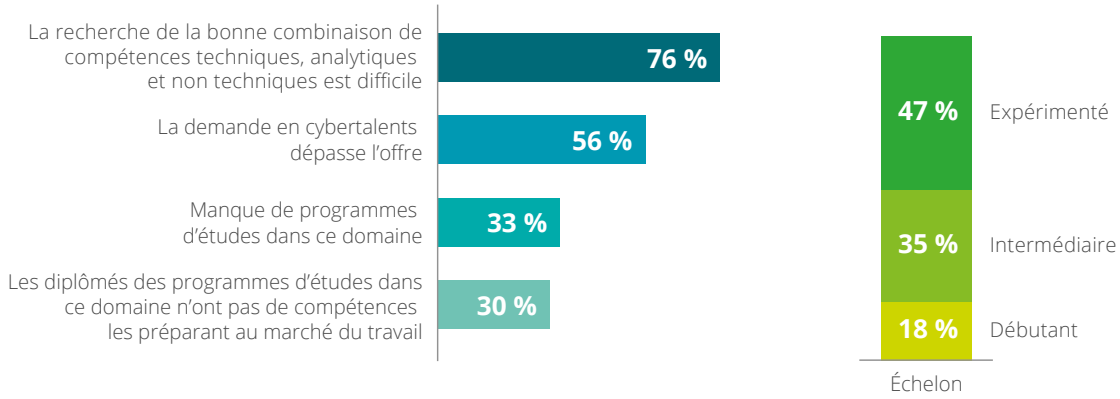


Figure 6 : Principaux défis pour le recrutement et difficulté selon l'échelon



Gestion du cycle de vie des talents

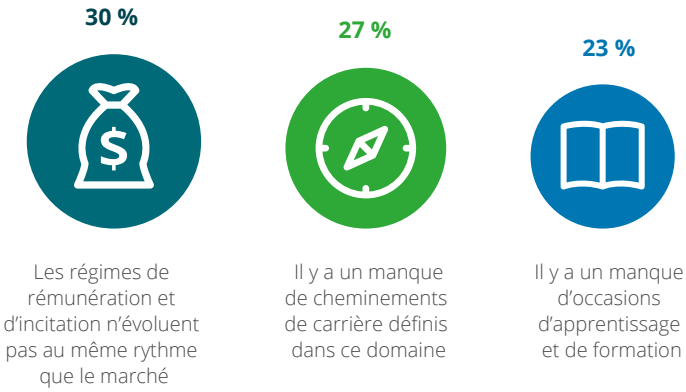
Le recrutement, le perfectionnement et la fidélisation des professionnels de la cybersécurité demeurent des défis constants. Selon notre sondage, il existe un certain nombre de problèmes précis :

Recrutement. Le principal défi de recrutement pour les organisations est de trouver la bonne combinaison de compétences techniques, analytiques et non techniques. (Voir la figure 6.)

Lorsqu'on leur a demandé d'évaluer la difficulté que pose le recrutement des cybertalents à différents échelons, les répondants ont souligné que le recrutement des employés expérimentés et intermédiaires était particulièrement difficile. (Voir la figure 6.)

Les difficultés de recrutement sont aggravées par le fait que, traditionnellement, l'accent était mis sur des compétences techniques très précises. Il en résulte des descriptions de poste de plus en plus ésotériques.

Figure 7 : Défis de perfectionnement et de fidélisation



Perfectionnement et fidélisation. Les régimes de rémunération et d'incitation n'évoluent pas au même rythme que le marché, ce qui nuit au recrutement et à la fidélisation de cybertalents qualifiés (cela englobe les talents d'autres secteurs de l'entreprise). Parmi les autres défis, mentionnons le manque de cheminements de carrière définis dans le domaine de la cybersécurité et un manque d'occasions d'apprentissage et de perfectionnement. (Voir la figure 7.)

Ces défis ne sont pas uniques au Canada. Dans un récent sondage, l'Enterprise Security Group a constaté que 66 % des professionnels de la cybersécurité à l'échelle mondiale n'ont pas de cheminement de carrière clairement défini ou de plan précis pour faire passer leur carrière au niveau supérieur. En outre, 60 % des répondants ont indiqué être seulement plutôt satisfaits ou insatisfaits à différents degrés du poste qu'ils occupent actuellement[6].

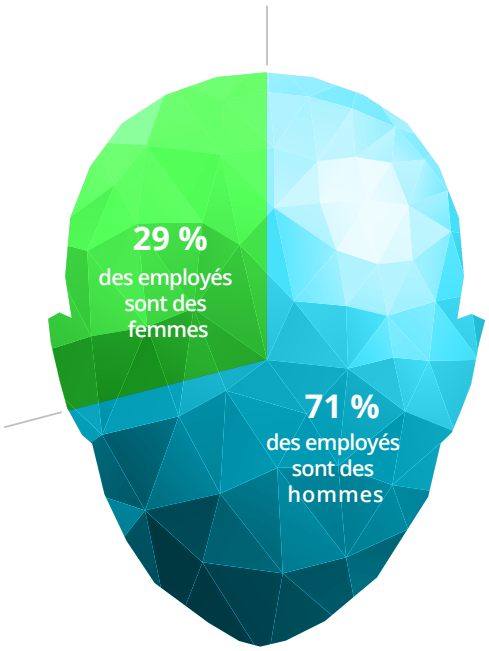
Si on les regroupe, les défis auxquels sont confrontées les entreprises canadiennes sur le plan du recrutement, du perfectionnement et de la fidélisation des cybertalents entraînent deux principaux effets : une capacité limitée d'embaucher les bonnes personnes au bon moment, et une main-d'œuvre transitoire, où les investissements dans le perfectionnement pourraient être entravés par les employés qui changent fréquemment d'entreprise.

Productivité

Il s'agit d'un secret de Polichinelle au sein de la communauté de la cybersécurité : la fonction de cybersécurité est confrontée à un important défi de productivité.

Une étude récente a révélé que, pour l'ensemble du Canada, les organisations consacrent environ 21 000 heures à enquêter sur des alertes de sécurité fausses ou erronées, ce qui représente un coût annuel d'environ 1,3 million de dollars[7]. Ce jeu du chat et de la souris est en partie un résultat de l'asymétrie entre les attaquants et les défenseurs : les attaquants n'ont qu'à réussir une seule fois pour causer des dégâts importants, alors que les défenseurs doivent réussir à tous les coups. Ce problème est également exacerbé par le fait qu'un chef de la sécurité de l'information doit généralement gérer plus de 70 outils de cybersécurité[8] dans un contexte où les affaires, les technologies et les fournisseurs sont en constante évolution. Le défi de productivité ne fera qu'augmenter à mesure que les organisations continueront d'investir dans des technologies avancées.

Figure 8 : Cybersécurité et genre au Canada



Inclusion

Les professionnels de la cybersécurité d'aujourd'hui ont tendance à être majoritairement des hommes et ont une expérience en informatique. Ce profil étroit laisse croire qu'une inclusion accrue pourrait représenter une solution potentielle encore inexploitée pour remédier à la pénurie de cybertalents.

Selon les résultats de notre sondage, les équipes de cybersécurité canadienne ne comptent en moyenne que 29 % de femmes. (Voir la figure 8.) À certains égards, il s'agit d'un résultat positif, car il est beaucoup plus élevé que la moyenne mondiale de 11 % [9]. Cependant, il reste encore une grande place à l'amélioration – en particulier au niveau de la direction. Notre recherche nous a permis de trouver seulement un petit nombre de femmes à la tête de grandes organisations de cybersécurité au Canada.

Les expériences monolithiques sont également répandues. Selon une étude du International Information Systems Security Certification Consortium (ISC^2), 70 % des professionnels de la cybersécurité en Amérique du Nord possèdent une expérience en informatique[10]. Bien que cela ne soit pas nécessairement un problème, cela limite artificiellement la réserve potentielle de talents et empêche éventuellement les nouvelles perspectives et réflexions. En outre, le profil de ces professionnels peut ne pas correspondre aux compétences et au savoir-faire dont les entreprises auront besoin pour effectuer une gestion efficace de la cybersécurité dans l'avenir.

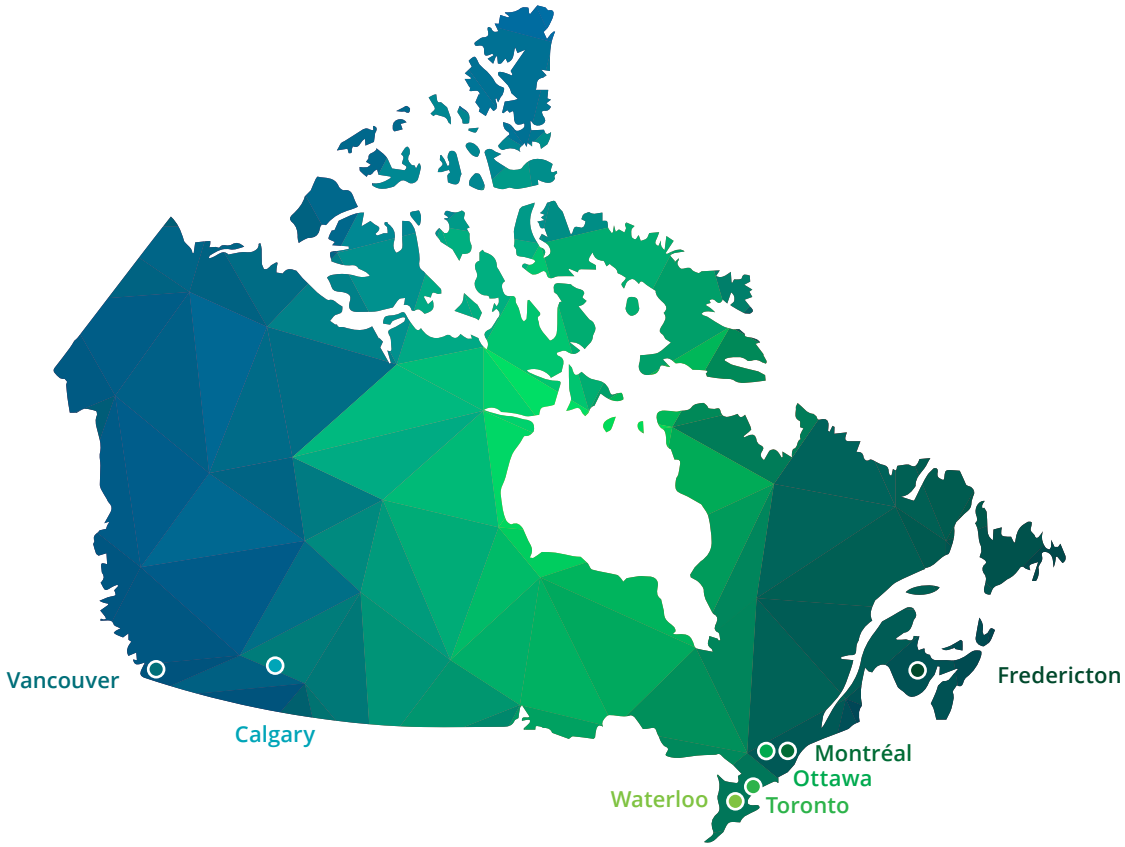
Établissements d'enseignement

L'éducation est une priorité pour les Canadiens. Notre pays possède un système d'éducation reconnu, et près des deux tiers des adultes canadiens ont terminé des études postsecondaires[11].

Dans le domaine de la cybersécurité, les établissements d'enseignement du Canada jouent un rôle important en tant que source naturelle de talents de cybersécurité. (Voir la figure 9.)

Le système d'éducation du Canada reconnaît le besoin de former les talents en cybersécurité, et les établissements de tous les niveaux prennent des mesures actives pour y arriver. Cependant, il reste encore des défis importants à relever.

Figure 9 : Centres universitaires de cybersécurité au Canada

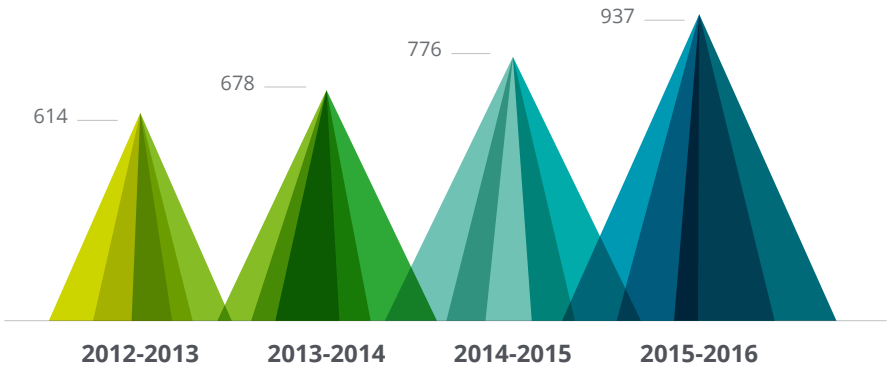


Les établissements collégiaux font des progrès, mais ont du mal à garder le rythme

Les établissements collégiaux ont réussi à répondre efficacement à la demande du marché – tant des employeurs que des étudiants – et forment activement la prochaine génération de cyberprofessionnels. Cette tendance s'observe partout au pays.

Par exemple, en Ontario seulement, le nombre d'étudiants inscrits dans les programmes axés sur la cybersécurité a augmenté de façon constante, totalisant presque 1 000 étudiants en 2015-2016[12]. (Voir la figure 10.)

Figure 10 : Inscription à des programmes collégiaux axés sur la cybersécurité (Ontario)



Source : Advanced Education and Skills Development, April 8, 2014, https://www.ontario.ca/data/college-enrolment

Cette augmentation du nombre d'inscriptions dans les programmes de cybersécurité représente environ 7 % de tous les étudiants inscrits dans des programmes collégiaux de TI en Ontario.

D'un océan à l'autre, les collèges s'efforcent de répondre à la demande accrue de formation en cybersécurité. Cependant, ils sont confrontés à un certain nombre d'obstacles importants. Selon notre groupe de discussion, le domaine de la cybersécurité évolue si rapidement que les formateurs ont du mal à maintenir leurs programmes d'études à jour. En effet, certaines compétences précises peuvent se transformer ou devenir obsolètes en un clin d'œil, en particulier dans le domaine de la cybersécurité, où les technologies et les cybermenaces évoluent à un rythme vertigineux. Paradoxalement, la pénurie de cybertalents rend difficile le recrutement de formateurs qualifiés qui pourront former un plus grand bassin de talents. Ces obstacles empêchent les établissements collégiaux de satisfaire pleinement les besoins du marché.

Les universités ont des forces sur lesquelles s'appuyer, mais des points de friction à éliminer

Les universités canadiennes sont performantes pour enseigner les sciences, les technologies, l'ingénierie et les mathématiques (STIM), et notre groupe de discussion a montré une forte demande des étudiants pour des programmes de cybersécurité au premier cycle et aux cycles supérieurs.

Un certain nombre d'universités accueillent des centres de recherche renommés et offrent des spécialisations en cybersécurité dans le cadre de programmes plus vastes. Par exemple, plus de 100 étudiants sont actuellement inscrits au volet de la sécurité informatique du programme d'informatique de l'Université Carleton, et ce nombre ne cesse de croître. Dans une perspective plus générale, l'organisation SERENE-RISC a catalogué 450 cours liés à la cybersécurité dans 60 universités au Canada en 2015[13]. Malgré ces constatations positives, quelques points de friction notables apparaissent au sein du secteur universitaire.

L'intégration des concepts de cybersécurité dans les programmes plus généraux d'informatique et de génie reste relativement faible, les cours de cybersécurité étant généralement considérés comme des cours facultatifs de fin de programme. Lorsque les concepts de cybersécurité sont intégrés, tels que le concept de validation en informatique, l'importance qui leur est accordée est faible compte tenu de la situation actuelle. Dans l'enseignement de l'ingénierie civile, par exemple, la sécurité est un élément de base du design.

Plus fondamentalement, le principal moteur des universités est de faire avancer la recherche et le progrès intellectuel, et non de répondre à la demande du marché. Ainsi, notre groupe de discussion a cerné un décalage perçu entre les incitatifs du secteur universitaire et ceux du secteur, ce qui se traduit par des points de friction

des deux côtés. Le secteur considère que trop peu d'efforts sont déployés pour la formation des diplômés en cybersécurité qui peuvent apporter une contribution immédiate à l'entreprise, tandis que les universités perçoivent un manque de soutien du secteur pour la recherche universitaire en cybersécurité.

La formation en cybersécurité doit commencer tôt

Un nombre croissant d'organisations au Canada et dans le monde commencent à offrir de la formation en cybersécurité aux élèves de la maternelle jusqu'à la fin du secondaire. Au Canada, parmi les efforts notables, mentionnons le programme CyberSmart[14] de CyberNB dans les écoles du Nouveau-Brunswick. Le Virtual Network and Cyber Security Centre de l'école secondaire Sisler cherche à préparer les élèves du secondaire de tout le Manitoba à entreprendre une carrière dans des domaines pour lesquels la demande est grande, comme les TI, la réseautique, la cybersécurité et la virtualisation. Israël et d'autres pays commencent à offrir de la formation sur la cybersécurité encore plus tôt.

Gouvernements

Les gouvernements de tous les paliers jouent un rôle important dans l'écosystème des talents en cybersécurité, non seulement parce qu'ils doivent retenir les services de cybertalents pour protéger les données et les systèmes publics, mais aussi parce qu'ils élaborent des politiques et des programmes pour remédier à la pénurie de talents.

Reconnaissance de l'importance de la cybersécurité

Le gouvernement du Canada a pris des mesures importantes pour reconnaître l'importance de la cybersécurité en s'engageant à investir 507 millions de dollars sur cinq ans dans le cadre de la nouvelle Stratégie nationale de cybersécurité énoncée dans le budget fédéral de 2018[15]. L'un des principaux objectifs de la stratégie est de construire un cyberécosystème innovant et adaptatif. Cela comprend une mesure visant à soutenir la création de jusqu'à 1 000 stages professionnels en cybersécurité[16].

À l'échelle provinciale, les initiatives dignes de mention comprennent l'organisme CyberNB susmentionné du Nouveau-Brunswick ainsi que l'investissement de 64 millions de dollars annoncé par le gouvernement de l'Ontario « afin d'améliorer les cyberpratiques existantes et d'attirer des spécialistes en forte demande du domaine de la cybersécurité en utilisant de nouvelles méthodes de recrutement, notamment par l'entremise de partenariats novateurs avec les établissements d'enseignement postsecondaire[17] ».

Bien que ces mesures soient positives, il faudra du temps pour que leur incidence sur l'écosystème des talents se fasse sentir. En outre, une grande collaboration entre les secteurs public et privé sera nécessaire afin d'assurer l'efficacité de ces mesures.

Résoudre aujourd'hui les problèmes de demain

L'un des principaux cyberdéfis pour les organisations est de recruter des talents expérimentés, et ce, dès maintenant. De plus, on constate que les lacunes actuelles liées aux cyberrisques sont de plus en plus occasionnées par les nouvelles technologies. Cela nous mène à définir un besoin à deux facettes :

1) faire croître le bassin de talents de manière inhabituelle par des voies telles que l'immigration qualifiée;

2) reconnaître les interdépendances entre les progrès technologiques et les cyberrisques et prendre les mesures qui s'imposent.

Les gouvernements fédéral et provinciaux jouent un rôle important dans ces deux domaines.

3 Les différents visages de la cybersécurité

Malgré les progrès réalisés dans les milieux des affaires, universitaires et gouvernementaux, il est clair que des défis persistants demeurent. Les efforts actuels ne sont pas suffisants pour surmonter la pénurie de cybertalents et combler les lacunes grandissantes liées aux cyberrisques.

Comme certains l'ont fait valoir, noyer le problème sous d'autres technologies n'est pas la solution.

Pour réussir, il faudra mener une nouvelle réflexion et adopter une nouvelle perspective ou, plus précisément, un nouveau cadre sur les cybertalents qui propose des façons nouvelles et novatrices de s'attaquer au problème en considérant ce dernier sous un angle humain.

Pour être efficace, ce cadre doit être stable et instructif. Il doit réunir les talents en groupes stables (axés sur les capacités durables plutôt que sur les compétences éphémères) et fournir un point de référence utile pour comprendre et planifier l'évolution des besoins en talents dans le contexte de l'évolution des technologies. Il doit également être compréhensible pour les personnes non initiées au domaine de la sécurité, rendant ainsi le secteur professionnel de la cybersécurité plus accessible et inclusif pour un public plus général.

Humaniser la cybersécurité

Notre modèle de cybertalents, qui s'inspire du cadre Cybersecurity Workforce Framework des États-Unis du National Institute of Standards and Technology's National Initiative for Cybersecurity Education[18], s'axe sur sept personnalités de la cybersécurité. (Voir la figure 11.)

Le modèle a trois composantes :

- **Personnalités.** Il s'agit de personnifications de l'ensemble des capacités qui s'appliquent à différentes fonctions de cybersécurité.
- **Capacités.** Il s'agit des capacités générales qui sont transférables entre les tâches et les environnements de travail, l'accent étant mis sur celles qui sont essentielles à chaque personnalité pour accomplir son travail.
- **Connaissances/compétences.** Il s'agit d'une liste abstraite de connaissances et de compétences nécessaires pour exécuter des tâches précises. Celles-ci sont moins tributaires de l'évolution du contexte que les expertises pointues et les formations sur une technologie particulière. Cependant, elles constituent la composante la moins durable du modèle.

Les personnalités ont été disposées sous forme de roue pour illustrer la relation qu'elles entretiennent les unes avec les autres. Les personnes qui sont côte à côte ont tendance à être plus similaires que celles qui se trouvent de l'autre côté de la roue. De plus, bien que chaque personnalité soit distincte, il est probable que les cyberprofessionnels s'identifieront à une personnalité en particulier, mais qu'ils auront aussi des affinités avec les personnalités voisines.

Figure 11: Les sept personnalités de la cybersécurité.

Pour demeurer stable, le cadre met l'accent sur des capacités transférables plutôt que sur des compétences précises. Bien que les compétences demeurent importantes, elles doivent rester au second plan plutôt que d'être au centre des préoccupations. Cela signifie qu'au lieu de centrer leurs efforts d'embauche et de formation sur des compétences techniques précises, les organisations canadiennes feraient mieux de considérer des « personnalités » plus générales ayant des capacités durables qui sont transférables à différents métiers et postes.

L'objectif du modèle est de servir de base pour mieux comprendre les dynamiques actuelles et futures relatives à la main-d'œuvre en cybersécurité, tout en facilitant la communication, l'éducation, le recrutement et la planification de la main-d'œuvre. En personnifiant les principaux ensembles de capacités, le modèle cherche à humaniser la discussion sur les cybertalents.

Stratège

Assure la gestion, l'orientation et la promotion des efforts en cybersécurité.

Capacités

- Influence
- Communication
- Leadership
- Incidence éthique

Connaissances et compétences

1. Sens des affaires
2. Politiques, considérations juridiques, réglementation
3. Architecture de la sécurité
4. Gestion des risques de sécurité

Rôles fréquents

- Chef de la sécurité de l'information
- Analyste en cyberstratégie
- Analyste de cyberpolitiques
- Analyste en cybercommunication
- Chef de cyberprogramme ou de cyberproduit

Conseiller

Fournit des conseils sur la conception et la création des systèmes et des réseaux sécurisés.

Capacités

- Esprit critique
- Raisonnement quantitatif
- Communication
- Influence

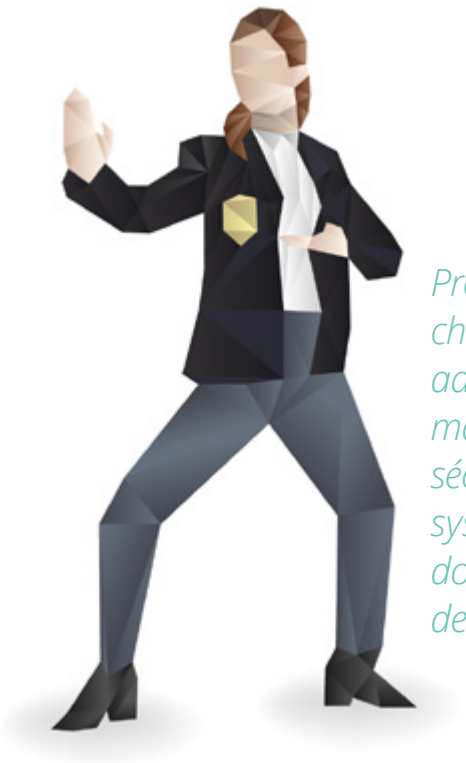
Connaissances et compétences

1. Gestion des risques de sécurité
2. Architecture de la sécurité
3. Politiques, considérations juridiques, réglementation
4. Sens des affaires

Rôles fréquents

- Architecte de la sécurité
- Analyste des risques de sécurité
- Analyste de la sécurité des applications

Défenseur



Prend en charge, administre et maintient la sécurité des systèmes, des données et des réseaux.

Capacités

- Jugement
- Collaboration
- État d'esprit axé sur les menaces

Connaissances et compétences

1. Sécurité de l'infrastructure
2. Administration des outils de sécurité
3. Gestion des risques de sécurité
4. Architecture de la sécurité

Rôles fréquents

- Analyste en sécurité des systèmes
- Administrateur de la sécurité

Pompier

Identifie, analyse et atténue les menaces pesant sur les systèmes internes, les données et les réseaux.

Capacités

- Souplesse
- Jugement
- Esprit critique
- État d'esprit axé sur les menaces

Connaissances et compétences

1. Gestion des incidents de sécurité
2. Administration des outils de sécurité
3. Sécurité de l'infrastructure
4. Administration des TI

Rôles fréquents

- Cyberanalyste
- Ingénieur en sécurité
- Intervenant en cas d'incident de cybersécurité
- Analyste en vulnérabilité
- Directeur du centre des opérations de sécurité

Bidouilleur

Exécute des activités spécialisées de détection des menaces et de tromperie délibérée pour cerner et atténuer les risques de cybersécurité.

Capacités

- État d'esprit axé sur les menaces
- Esprit critique
- Créativité
- Incidence éthique

Connaissances et compétences

1. Test de pénétration
2. Informatique judiciaire
3. Sécurité de l'infrastructure
4. Modélisation des menaces

Rôles fréquents

- Cyberopérateur
- Chasseur de menaces

Scientifique

Effectue une analyse spécialisée des renseignements sur les menaces, des données cryptographiques et de l'information sur la sécurité pour améliorer la posture de sécurité.

Capacités

- Esprit critique
- Raisonnement quantitatif
- État d'esprit axé sur les menaces

Connaissances et compétences

1. Analyse des renseignements
2. Science des données
3. Cryptographie

Rôles fréquents

- Analyste des données sur les menaces
- Directeur de la cyberanalyse

Détective

Enquête sur les atteintes à la cybersécurité ou les infractions liées aux systèmes, aux réseaux et aux preuves numériques.

Capacités

- État d'esprit axé sur les menaces
- Esprit critique
- Conscience sociale
- Incidence éthique

Connaissances et compétences

1. Informatique judiciaire
2. Gestion des incidents liés à la cybersécurité

Rôles fréquents

- Analyste en cybercriminalistique

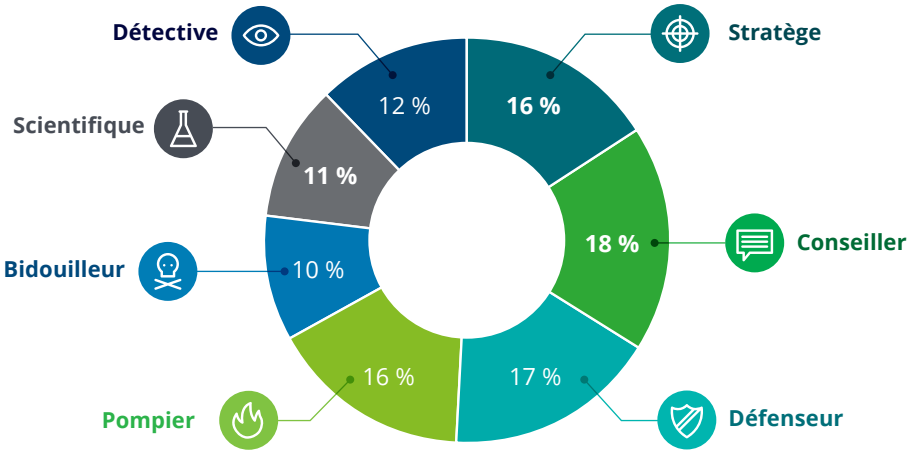
L'avenir sera différent

Nous avons vu comment les lacunes liées aux cyberrisques entraînent, d'un point de vue quantitatif, une demande accrue de professionnels de la cybersécurité. En considérant sous un angle humain le défi du Canada en ce qui concerne les talents en cybersécurité, nous pouvons mieux comprendre comment il évolue selon une perspective qualitative.

Les résultats de l'enquête révèlent que la cybermain-d'œuvre actuelle du Canada reflète en grande partie l'évolution de la cybersécurité dans le contexte des infrastructures et des opérations – l'accent est mis sur les rôles visant à protéger les composantes de l'infrastructure ainsi qu'à détecter les menaces ordinaires et à intervenir en conséquence. Cependant, au cours des trois à cinq prochaines années, les répondants au sondage s'attendent à ce que les personnalités moins conventionnelles – comme le stratège et le scientifique – revêtent une plus grande importance. (Voir la figure 12.)

Malheureusement, les répondants au sondage s'attendent également à ce que les personnes qui correspondent à ces deux personnalités soient les plus difficiles à trouver et à recruter.

Figure 12 : Composition de la cybermain-d'œuvre canadienne



Personnalités les plus difficiles à trouver aujourd'hui : Stratège, Scientifique

Personnalités dont l'importance augmentera le plus : Stratège, Scientifique, Conseiller

À mesure que les entreprises et les modèles de mise en œuvre des technologies évoluent, les conseillers continueront de jouer un rôle de premier plan. Dans notre sondage, ils sont classés comme les professionnels de la cybersécurité que l'on rencontre le plus fréquemment de nos jours, ainsi que l'une des personnalités dont l'importance augmentera le plus dans l'avenir. Cependant, le rôle précis d'un conseiller est appelé à évoluer; une expérience pratique des outils émergents (p. ex., la virtualisation, la conteneurisation, l'infonuagique) deviendra de plus en plus importante.

Pour tirer le meilleur parti des plus récentes technologies, une expertise technique approfondie sera nécessaire dans des domaines tels que la science des données, l'intelligence artificielle et l'apprentissage machine – en conséquence, un grand nombre de scientifiques devront répondre à l'appel.

La définition du problème à résoudre continue d'être un défi pour de nombreux cyberexperts dont les compétences sont purement techniques. Par exemple, nous avons constaté qu'un nombre croissant d'organisations ont de la difficulté à améliorer leurs capacités en science des données et en analyse dans le domaine de la cybersécurité parce qu'elles n'ont pas de perspective et de contexte stratégique. En outre, au fur et à mesure que la fonction de cybersécurité évolue, il deviendra essentiel d'apprendre à se conformer à des exigences réglementaires de plus en plus strictes et à communiquer efficacement les cyberrisques à l'entreprise. Cela entraînera un besoin accru en stratèges.

La double nécessité de posséder, d'une part, un sens stratégique des affaires et, d'autre part, une expertise technique approfondie met probablement en évidence le besoin de prévoir l'évolution du domaine de la cybersécurité au cours des trois à cinq prochaines années. Cela suggère également qu'il faille créer des partenariats interfonctionnels entre les personnalités.

Au fil du temps, il est fort probable que d'autres personnalités évoluent en raison de technologies perturbatrices telles que l'automatisation des processus robotisés, l'intelligence artificielle et l'infonuagique. Pour les défenseurs, cela pourrait se traduire par une réduction du nombre d'évaluations de contrôle à effectuer, grâce à l'automatisation et à l'intelligence artificielle, ainsi que par une transition vers des services gérés dans le nuage.

Pendant ce temps, les pompiers seront amenés à devenir des scientifiques, à mesure que les tâches d'analyse de niveau inférieur s'automatiseront.

4 Recommandations et prochaines étapes

Le fait de considérer l'écosystème canadien des cybertalents sous un angle humain permet de révéler des mesures essentielles que devront prendre à la fois les établissements d'enseignement, les gouvernements et les entreprises, afin de renforcer notre atout concurrentiel sur la scène mondiale en exploitant en toute sécurité la pleine puissance et le plein potentiel des technologies émergentes. Pour y parvenir, il faudra prendre des mesures audacieuses afin de surmonter la pénurie de talents en cybersécurité et de combler les lacunes liées aux cyberrisques.

Stratégie et culture

Pour surmonter la pénurie de cybertalents et s'attaquer efficacement aux cyberrisques, il faudra mettre au point une stratégie de talents innovante, inscrite dans une culture cohérente et soutenue par une infrastructure humaine et technologique.

Lorsqu'elles essaient d'attirer et de fidéliser des cybertalents, de nombreuses organisations adoptent des tactiques précises (pensons aux marathons de programmation ou aux programmes de travail flexibles), mais elles laissent de côté leur stratégie globale de talents et oublient qu'il est primordial de construire un modèle de talents durable.

La stratégie de cybertalents d'une organisation aide à définir et à uniformiser un ensemble diversifié de stratégies de ciblage des talents. Elle permet ainsi d'avoir un plan lui permettant d'accéder à des talents rares et de les mobiliser tout au long du cycle de vie des talents. Si votre organisation est prête à transformer son approche en matière de cybertalents, commencez par prendre en considération les éléments clés suivants :

Vision

Votre vision de la cybersécurité dictera la structure de votre organisation ainsi que les capacités, les compétences et les comportements que vous devez acquérir. Chaque organisation pourra compter sur une combinaison unique de personnalités décrites dans le cadre sur les talents. Par exemple, la transition d'un programme de sécurité axé sur les technologies et les TI vers un programme où la cybersécurité est intégrée à l'ensemble de l'organisation nécessitera un modèle de talents différent et, éventuellement, un ensemble différent de compétences. Pour effectuer une telle transition, les organisations de cybersécurité doivent s'éloigner des modèles hiérarchiques en éliminant les différents niveaux et en confiant la responsabilité aux personnes touchées le plus directement par les décisions. Un plus grand accent doit être mis sur la responsabilisation, la communication, la collaboration ainsi que la connaissance et l'appréciation du monde des affaires.

Les employeurs du secteur des services financiers s'unissent pour accroître le bassin de talents

La Toronto Financial Services Alliance (TFSA) a mis au point une stratégie coordonnée liée aux talents en cybersécurité dans le but d'accroître de façon notable le bassin de talents dans le secteur des services financiers de la région de Toronto grâce à des investissements ciblés. Un groupe de travail formé de différents employeurs a commencé récemment à établir la priorité en ce qui a trait à l'élaboration et à l'exécution d'initiatives relatives aux talents en cybersécurité à l'échelle du secteur. La première étape consiste à collaborer avec les établissements d'enseignement dans le but de créer un programme d'études supérieures en cybersécurité qui répondrait mieux aux besoins sectoriels.

« La pénurie de talents spécialisés en cybersécurité a des répercussions sur l'ensemble des employeurs du secteur des services financiers, et la demande pour les talents dépasse les initiatives de recrutement individuelles. En participant à la stratégie liée aux talents en cybersécurité de la TFSA, nos membres peuvent exercer leurs activités de manière plus stratégique afin de trouver des solutions qui combleront les lacunes », a déclaré Sashya D'Souza, vice-présidente principale des initiatives en matière de talents de la TFSA.

Proposition de valeur en matière de talents

La prochaine étape consiste à articuler une proposition de valeur en matière de talents qui correspond à votre vision. Votre stratégie de talents vous aidera à déterminer la qualité et le type de talents requis. La proposition de valeur en matière de talents doit répondre à la question suivante : « Qu'offrez-vous à vos talents pour les inciter à poursuivre leur carrière au sein de votre organisation? »

Aspects à prendre en compte :

- Cheminements de carrière définis
- Possibilités de formation formelles et informelles
- Incitatifs et rémunération
- Portée du travail, expérience et compétences acquises
- Structure des équipes et accès à des leaders techniques, stratégiques et d'affaires

Proposition de valeur en matière de talents de Deloitte

En tant qu'entreprise de services professionnels, nous savons que nos gens sont notre atout le plus précieux. Pour continuer à attirer les meilleurs talents, nous nous sommes donné la mission de comprendre *pourquoi* nos gens avaient choisi Deloitte et, lorsqu'il s'agit de choisir un employeur, *ce qu'ils considèrent* comme les éléments déterminants de l'expérience talent. Nous appelons cela notre proposition de valeur en matière de talents.

« Le vrai leadership du marché dépend de nos employés, et nous savons que nos employés ont des choix », affirme Norma Kraay, associée directrice, Talent, de Deloitte Canada. « Notre proposition de valeur en matière de talents constitue le fondement de l'expérience talent d'un employé chez Deloitte. Ce sont les promesses que nous faisons à chaque employé, et que nous nous faisons les uns aux autres, et ce, tous les jours. »

Lacunes liées à la main-d'œuvre

La collecte de données sur votre main-d'œuvre actuelle vous permet de cerner et de corriger de manière réfléchie et efficace les lacunes en matière de capacités, de compétences et de comportements

Les données clés sur les domaines de travail, les compétences et les lacunes vous permettent de prendre des décisions stratégiques sur de nouvelles façons d'aborder le travail.

- Certains flux de travail pourraient-ils être mieux gérés au moyen d'une impartition ou de services gérés?
- Peut-on tirer profit des technologies cognitives et de l'automatisation (p. ex., la détection automatique des menaces) pour réduire la participation humaine?
- Certaines compétences peuvent-elles être combinées de nouvelles façons pour résoudre des problèmes difficiles et favoriser l'innovation?

La création d'un plan pour redéfinir le travail et maximiser les ensembles de compétences existants permet aux cybertalents, si peu nombreux, de se concentrer sur des activités qui nécessitent une expertise humaine, comme la compréhension du profil de risque global de l'entreprise et la définition des priorités en leadership. De nombreuses organisations de sécurité se fondent sur les dernières meilleures pratiques du secteur du développement de produits et de logiciels et organisent leurs activités autour d'objectifs partagés et non de fonctions, c'est-à-dire en combinant divers groupes de personnes (p. ex., des stratèges et des scientifiques) et en leur donnant un objectif commun à atteindre.

Nouveaux modèles de talents

Les modèles de talents non traditionnels peuvent vous aider à tirer le meilleur parti des ressources limitées en cybersécurité. Par exemple, vous pouvez créer une organisation agile fondée sur des modèles de main-d'œuvre « à la demande » qui privilégient le recours à des travailleurs occasionnels pour soutenir les activités lorsque les capacités requises fluctuent (p. ex., évaluation des risques des fournisseurs et évaluations des risques liés à des technologies et à des projets émergents). Vous pouvez également tirer parti d'innovations telles que l'externalisation ouverte pour obtenir rapidement de l'information globale sur des problèmes ou pour acquérir des connaissances spécialisées dans des secteurs clés.

Analytique des données

Au sein d'un cyberenvironnement complexe et en rapide évolution, le fait de mobiliser la puissance de l'analytique des données pour s'attaquer aux défis liés aux cybertalents devrait constituer une pratique opérationnelle habituelle.

Tout comme les entreprises utilisent actuellement les données sur les clients pour concevoir des expériences et des produits répondant mieux aux besoins et aux désirs de leurs clients, les entreprises de cybersécurité avant-gardistes peuvent utiliser l'analytique des données pour déceler les tendances en matière de talents, les lacunes et les percées technologiques leur permettant de prendre des décisions plus éclairées.

Les plus récentes capacités d'analytique des talents peuvent faciliter l'adoption d'une nouvelle approche pour la planification de la main-d'œuvre et changer la donne en ce qui concerne la prévision des besoins en talents, la schématisation des catégories d'emplois, l'anticipation des redondances et la prédiction de l'offre et de la demande en talents.

Culture et marque en matière de talents

Pour exécuter et pérenniser votre vision, déterminez les valeurs que vous considérez comme les plus importantes pour votre main-d'œuvre et votre stratégie, et alignez-les dans l'ensemble de votre entreprise et de vos opérations. Cela étant dit, n'oubliez pas que, de nos jours, les meilleurs talents veulent exécuter du travail constructif et les organisations ont tout intérêt à souligner l'importance de la fonction de cybersécurité.

Créez et personnifiez activement une culture et une marque qui cadrent avec la main-d'œuvre de cybertalents que vous ciblez.

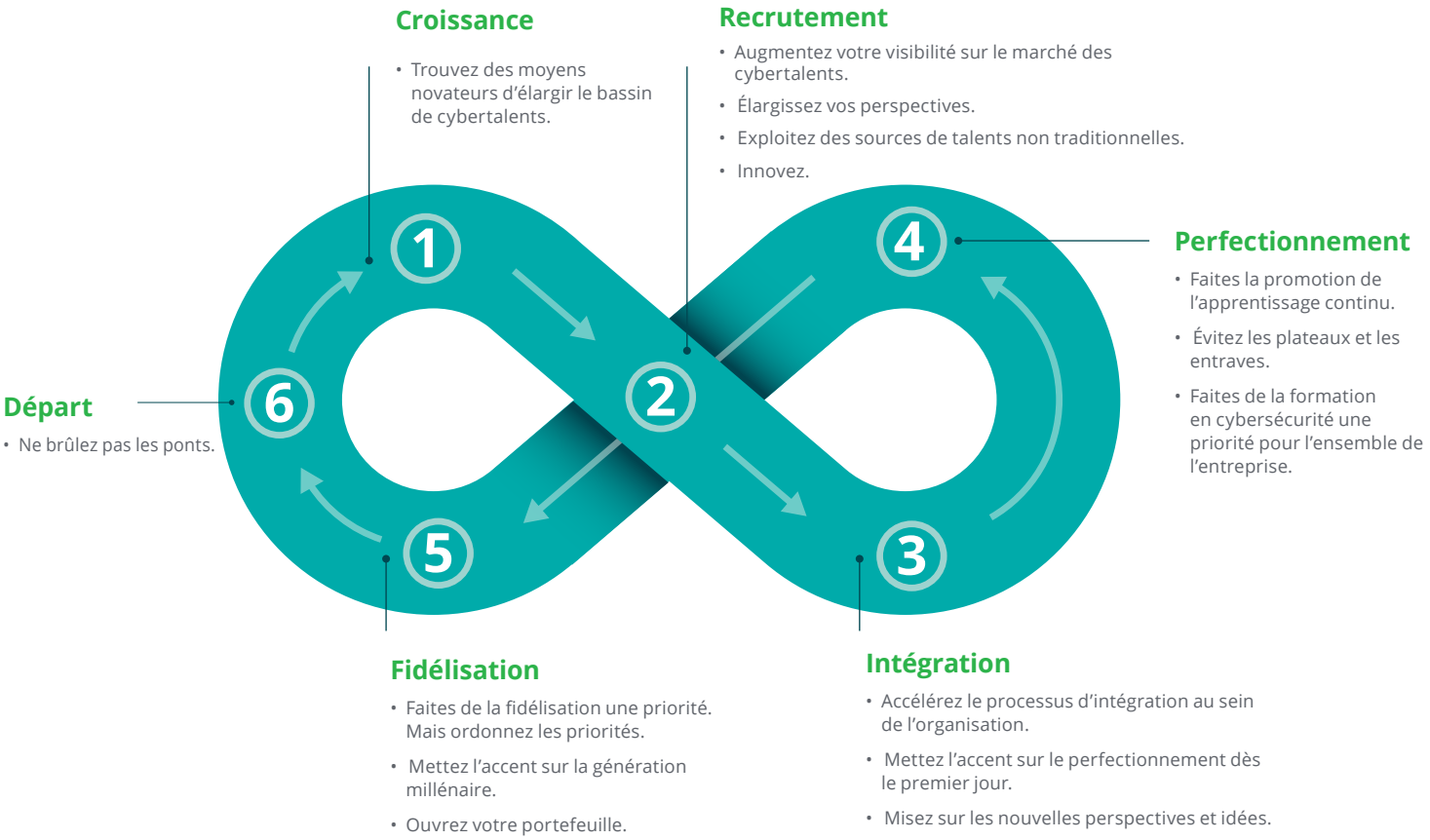
Augmentez votre compétitivité en offrant un salaire concurrentiel, la liberté d'avoir une influence et l'autonomie d'effectuer son travail. Prenez des décisions difficiles en matière de rendement le plus tôt possible afin d'éviter d'avoir à gérer des compétences et des comportements incompatibles.

Favorisez l'engagement personnel en fournissant du travail constructif, un environnement de travail positif où règne la confiance, des pratiques et des comportements de gestion efficaces ainsi que des occasions de croissance et de développement.

Le cycle de vie des talents

Un moyen efficace d'opérationnaliser votre programme de cybertalents est de l'axer sur le modèle du cycle de vie des talents : croissance, recrutement, intégration, perfectionnement, fidélisation et départ. (Voir la figure 13.)

Figure 13 : Modèle du cycle de vie des talents



Croissance

Trouvez des moyens novateurs d'élargir le bassin de cybertalents. Chaque organisation doit assumer une certaine responsabilité pour répondre au défi des cybertalents en déployant ses efforts dans l'ensemble de l'écosystème afin de faire croître le futur bassin de talents. Cela comprend d'enseigner aux jeunes les pratiques à suivre et les risques liés à la cybersécurité et de susciter un intérêt à l'égard d'une carrière dans ce domaine, et ce, dès aujourd'hui.

De nos jours, nous faisons la promotion auprès des jeunes de l'importance d'une formation en STIM ainsi que des cheminements de carrière dans ces domaines. Bien que ce travail soit essentiel, il faut également chercher les futurs talents en dehors des programmes des STIM. Les différentes personnalités du cadre sur les cybertalents possèdent différentes compétences et expériences. Ces talents seront de plus en plus issus des domaines non liés aux STIM : les stratèges et les conseillers ont des compétences qui viennent compléter celles plus techniques des scientifiques et des détectives

Former les jeunes en STIM, robotique et en programmation informatique

Il y a de fortes chances que vos enfants occupent plus tard des emplois qui n'ont pas encore été inventés. Au Canada et ailleurs dans le monde, on assiste à un virage fondamental vers la « numérisation » et l'utilisation de l'intelligence artificielle, de la robotique et d'autres technologies de pointe pour transformer les entreprises de tous les secteurs. De nouveaux emplois sont créés alors que d'autres sont éliminés. Chez les consommateurs, la domotique, les technologies prêt-à-porter et les robots programmables transforment notre façon de jouer et de passer notre temps.

Envision Robotics aide les enfants à acquérir des compétences pertinentes au 21e siècle grâce à un programme fondé sur les STIM qui allie robotique et programmation. Armés de ces compétences, les enfants seront mieux préparés pour un avenir où les possibilités sont infinies. « Des programmes comme le nôtre sont essentiels pour aider le Canada à combler les lacunes en matière de compétences nationales et à demeurer concurrentiel sur la scène mondiale », affirme John MacKinnon, fondateur d'Envision Robotics.

Le fait d'exposer les jeunes en plein épanouissement à ces domaines stimulants le plus tôt possible peut aider à façonner leurs intérêts et à influencer positivement leurs choix de carrière.

Voici quelques initiatives novatrices de partout dans le monde qui contribuent à accroître l'offre en cybertalents :

- En Israël, l'enseignement des STIM et de la cybersécurité aux enfants est une mission nationale.
- Aux États-Unis, les Éclaireuses ont lancé de nouveaux badges en robotique et en cybersécurité.
- De nouvelles entreprises en démarrage comme Envision Robotics enseignent aux enfants les principes des STIM, de la robotique et de la programmation informatique.
- Deloitte et CoderDojo ont mis sur pied une communauté de clubs de programmation pour les enfants de 7 à 17 ans.
- Le programme picoCTF de l'Université Carnegie Mellon vise à éduquer les étudiants du secondaire sur l'importance de la cybersécurité.
- Le programme Safe and Secure Online d'(ISC²) offre des ressources pour les formateurs, les dirigeants et les bénévoles pour enseigner la cybersécurité à la communauté.
- La University College London permet aux jeunes filles d'acquérir des compétences en codage et en développement d'applications et de jeux ainsi que les bases de la cybersécurité.

Améliorer l'éducation pour rester en phase avec l'évolution des cyberrisques

Polytechnique Montréal et Deloitte ont uni leurs forces pour réorganiser le programme de formation de haut niveau de la Polytechnique dans le domaine de la cybersécurité. Le contenu des cours des trois programmes de certification en cyberenquête, en cyberfraude et en cybersécurité a été amélioré pour tenir compte des besoins actuels du marché et de la nature changeante des cybercrimes.

« Le partenariat entre la Polytechnique et Deloitte permet aux étudiants d'avoir accès à des conférenciers qui ont une expérience concrète de la cybersécurité et qui sont parmi les meilleurs spécialistes de la cybercriminalité au monde », déclare Amir Belkhelladi, associé leader, Service des risques d'entreprise de la région de l'Est chez Deloitte. « À mesure que les cybercriminels affinent leurs méthodes, les organisations doivent prendre des mesures pour veiller à ce que leur personnel affecté à la cybersécurité demeure à l'affût des plus récentes menaces et des moyens de les contrer. D'où l'importance des programmes de formation offerts par la Polytechnique. »

Parmi les autres occasions d'élargir le bassin de cybertalents, mentionnons les suivantes :

- Fidéliser des personnes déjà sur le marché du travail et permettre leur transition vers un poste en cybersécurité (p. ex., le certificat en cybersécurité de l'école de formation continue de l'Université York).
- Accroître la présence féminine dans le domaine de la cybersécurité en collaborant avec les écoles, les universités et les recruteurs pour encourager les femmes à poursuivre une carrière dans les technologies, et en leur donnant accès à des modèles et à des possibilités égales.
- Construire un écosystème local de cybersécurité composé de formateurs et d'employeurs dans le but de réinventer l'expérience de formation en cybersécurité pour harmoniser l'apprentissage avec les besoins du secteur en matière de compétences.
- Parrainer des chaires de recherche dans des universités et collaborer avec des établissements collégiaux et universitaires afin d'élaborer et d'offrir des certificats d'études supérieures et des programmes de maîtrise professionnelle.
- Travailler avec les universités pour créer des cours de cybersécurité ou améliorer les cours existants, et favoriser la collaboration entre le secteur, le milieu universitaire et le gouvernement pour adapter les programmes d'études.

Collaborer afin de réinventer la cyberéducation et de bâtir un écosystème canadien de cybersécurité

La ville de Brampton et la province de l'Ontario collaborent avec l'Université Ryerson et le Collège Sheridan afin de créer un campus postsecondaire à Brampton. On y trouvera un centre national de cybersécurité, un pôle d'innovation pour connecter les étudiants avec d'autres organisations de la région ainsi qu'un centre pour l'éducation, l'innovation et la collaboration.

« Cette collaboration révolutionnaire entre le monde universitaire et les secteurs public et privé contribue à la création d'un centre national de cybersécurité », mentionne Nick Galletto, leader, Services liés aux cyberrisques de Deloitte Canada. « Notre Cabinet est fier de fournir sa part d'efforts en aidant à créer un centre de cybersécurité qui favorisera le développement de cybersolutions et la formation des générations futures de cybertalents. »

Investir dans la cyberéducation et la cyberrecherche de pointe

La Banque Royale du Canada (RBC) ouvre un laboratoire de cybersécurité et investit 1,78 million de dollars pour financer la recherche en informatique et l'innovation à l'Université de Waterloo.

Le financement appuiera de la cyberrecherche en informatique, en mathématiques et en cybersécurité. Les principaux domaines d'intérêt comprennent l'utilisation de l'apprentissage machine et de l'intelligence artificielle pour détecter et atténuer les menaces à la sécurité, la mise au point de technologies pour améliorer la sécurité et la confidentialité des données sur les consommateurs, et la création de méthodes de chiffrement robustes qui ne peuvent pas être déchiffrées par l'informatique quantique[19].

Financer la recherche pour lutter contre les cyberrisques touchant les services financiers

La Banque Scotia fait don de deux millions de dollars à l'Université de la Colombie-Britannique (UBC) pour financer la recherche liée à la cybersécurité. Au cours des cinq prochaines années, l'initiative de cybersécurité et d'analyse des risques de la Banque Scotia soutiendra divers projets de recherche et d'éducation – notamment des stages, des conférences et des marathons de programmation – afin de permettre une meilleure compréhension des cybermenaces qui pèsent sur le secteur des services financiers et d'aider au développement des outils et des talents nécessaires à la gestion des cyberrisques.

L'initiative de cybersécurité et d'analyse des risques de la Banque Scotia à l'UBC permettra à l'ensemble du secteur de mieux comprendre comment protéger ses actifs numériques. Parallèlement, le soutien de la Banque Scotia contribuera à la recherche et incitera les étudiants à recourir à la modélisation financière pour faciliter la gestion des risques et améliorer la protection des clients[20].

Recrutement

Augmentez votre visibilité sur le marché des cybertalents. Tirez parti de la proposition de valeur globale de votre entreprise afin d'établir votre « marque » d'employeur de choix pour les cybertalents. Faites la promotion de la cybersécurité en tant que profession – et de votre organisation en tant que milieu de travail idéal pour les cyberprofessionnels – en offrant des séances d'apprentissage et des démonstrations.

Élargissez le bassin. Comme il a déjà été indiqué, la grande majorité des professionnels de la cybersécurité commencent leur carrière dans d'autres fonctions liées aux TI. Ce parcours professionnel va probablement se diversifier à mesure que des technologies telles que l'automatisation, l'intelligence artificielle, l'apprentissage machine et l'infonuagique réduisent le besoin de faire appel à des professionnels des TI traditionnels.

Bien que les scientifiques, les défenseurs, les pompiers et les bidouilleurs aient besoin de compétences techniques spécialisées pour exercer leurs fonctions, d'autres personnalités, telles que les stratèges et les conseillers, doivent posséder des capacités dépassant les aspects techniques, telles qu'un esprit critique, une capacité d'influence, un état d'esprit axé sur les menaces et des compétences en analyse quantitative. En effet, 76 % des répondants indiquent qu'il est difficile de trouver la bonne combinaison de compétences analytiques et générales.

Élargir le bassin de talents afin d'engager plus tôt les talents qui ne sont pas dans le programme STIM et les talents en milieu de carrière avec les compétences fondamentales requises permettra d'améliorer la diversité sur le plan de la réflexion, de l'expérience, de la culture et du genre, ce qui favorisera l'innovation au sein des équipes de cybersécurité.

Les partenariats avec les nouveaux diplômés des programmes de gestion des risques, de sciences politiques, de droit et d'administration des affaires (MBA) se traduiront par un plus grand bassin de nouveaux talents possédant des compétences en réflexion critique, en analyse quantitative et en leadership.

Accueillez les professionnels réorientant leur carrière. Les stratèges et les conseillers sont de plus en plus sollicités, mais il faut du temps pour que ces nouveaux talents atteignent les échelons supérieurs. On peut toutefois combler plus rapidement cette lacune en misant sur les capacités et les compétences des personnes qui réorientent leur carrière, ce qui a également pour effet d'accroître la diversité et le niveau d'expérience des équipes.

Les candidats les plus prometteurs comprennent les professionnels en milieu de carrière occupant des fonctions internes telles que la gestion des risques d'entreprise et informatiques, l'audit interne, la gouvernance, la stratégie et la gestion des parties prenantes. Vous devrez investir dans la formation technique pour ces recrues internes, mais celles-ci auront une grande maturité et connaîtront bien le fonctionnement de votre environnement, une compétence importante qui leur permettra de gravir plus rapidement la courbe d'apprentissage.

De plus, l'intégration des professionnels en réorientation de carrière constitue un moyen de plus d'augmenter le nombre de femmes dans les équipes de cybersécurité.

Programmes de rotation pour le développement des meilleurs talents

La Sun Life offre cinq Programmes de rotation axés sur le développement du leadership permettant à des diplômés nouvellement embauchés triés sur le volet d'occuper par rotation différents postes au sein de l'entreprise. Ces programmes, qui vous amènent généralement à travailler dans divers établissements au Canada, donnent à des candidats prometteurs occupant des postes de leadership la possibilité de perfectionner leur connaissance du secteur des services financiers ainsi que de mieux évaluer et définir leurs objectifs de carrière.[21]

Exploitez des sources de talents non traditionnelles. Pour combler vos besoins en cybertalents, élargissez votre pipeline de recrutement en faisant appel à des populations inexploitées et en utilisant de nouvelles méthodes de recrutement, par exemple en vous tournant vers les programmes de placement des anciens combattants et d'autres personnes d'expérience issues des forces armées. En outre, certains travailleurs ayant de l'expérience technique et une formation non traditionnelle pourraient également être des candidats de choix pour le domaine de la cybersécurité. Il faut embaucher en tenant compte de la capacité d'apprentissage plutôt qu'en fonction d'un ensemble de compétences purement techniques.

Créez de nouveaux partenariats en faisant appel aux organismes gouvernementaux, aux établissements d'enseignement et aux programmes universitaires de votre région. Étendez la recherche de talents aux collèges communautaires, aux écoles techniques privées et à d'autres programmes de formation, puisqu'un nombre croissant de ces établissements offrent des programmes de cybersécurité, mais sont ignorés par les employeurs.

Innovez. Les descriptions de poste traditionnelles et les offres d'emploi en ligne peuvent constituer un moyen passif et inefficace pour attirer la variété de talents nécessaires.

En vous fondant sur le cadre sur les cybertalents et les personnalités, travaillez en collaboration avec des équipes internes et des responsables de l'embauche pour documenter les capacités, les attributs et les compétences dont votre organisation a besoin, à l'heure actuelle et dans l'avenir.

Déterminez quelles capacités sont obligatoires et quelles compétences peuvent être acquises au moyen d'une formation.

Attirez des candidats non traditionnels en affichant des offres d'emploi qui annoncent un arrangement sur le plan des compétences requises et de la formation offerte. Par exemple : « Si vous avez ces compétences de base, nous vous enseignerons ces compétences avancées. » Décrivez ensuite le parcours professionnel prévu une fois les nouvelles compétences maîtrisées.

Essayez d'autres approches novatrices et actives, telles que des partenariats avec des groupes universitaires en vue d'organiser des « marathons de programmation » axés sur la cybersécurité, dont les gagnants se verront accorder un poste au sein de votre entreprise.

Cette interaction concrète avec les étudiants permet d'établir très clairement leur savoir-faire et vous permet de tester leurs compétences spécialisées et générales. De tels événements peuvent donc être un moyen efficace de repérer de nouveaux talents et de perfectionner leurs compétences en cybersécurité.

Intégration

Accélérez le processus d'intégration de votre organisation. Compte tenu de la pénurie de professionnels de la cybersécurité qualifiés, il est important de soutenir et de mobiliser les nouveaux employés dès qu'ils se joignent à votre équipe. Intégrez rapidement vos nouvelles recrues à votre écosystème global en les présentant aux groupes externes à la cybersécurité, tels que les équipes de développement d'applications et de gestion des actifs numériques, pour les faire connaître et leur permettre de se constituer un réseau.

Mettez l'accent sur le perfectionnement dès le premier jour. En plus d'avoir de solides programmes d'intégration, les employeurs devraient rapidement offrir des possibilités de mentorat, d'affectation en rotation et d'observation de collègues plus expérimentés. Établissez un plan de carrière pour tous les cybertalents, et envisagez d'offrir un programme de perfectionnement en gestion permettant aux employés de travailler en rotation dans différents secteurs de l'entreprise.

Misez sur les nouvelles perspectives et idées. Affectez les nouveaux employés à une variété de projets, et incitez-les à explorer de nouvelles technologies et de nouveaux processus. Vous favoriserez ainsi leur perfectionnement professionnel, leur permettrez de prouver immédiatement leur valeur et permettrez à l'équipe de bénéficier d'une nouvelle perspective.

Perfectionnement

Favorisez l'apprentissage continu. La cybersécurité est un domaine très dynamique qui nécessite un apprentissage et un perfectionnement continuels. Investissez dans les employés pour les inciter à considérer la cybersécurité comme une carrière et non seulement comme un emploi. Aidez-les à développer et à parfaire leurs compétences en leur donnant l'occasion de se tenir à jour; encouragez-les à s'inscrire à des cours et à des conférences, et à obtenir des certifications. Jumelez les cybertalents avec des pairs occupant des fonctions associées à une personnalité adjacente du cadre afin de leur permettre de diversifier leurs compétences et leurs apprentissages. Favorisez l'innovation et la créativité en permettant aux personnes de consacrer du temps à des projets qui les intéressent personnellement.

Évitez les plateaux et les entraves. Alors que certains professionnels de la cybersécurité se consacrent principalement à l'amélioration de leurs compétences techniques, beaucoup sont à la recherche de nouveaux défis et de nouvelles façons de faire progresser leur carrière. En commençant par les rôles de premier échelon, définissez clairement les cheminements de carrière et les délais prévus pour l'avancement. Offrez des programmes de rotation et des occasions de partenariat avec d'autres fonctions pour exposer les talents à d'autres réalités et leur permettre d'acquérir de l'expérience. Offrez-leur du coaching intensif, des responsabilités qui leur permettent de se dépasser, du mentorat formel et informel et des occasions de mentorat inversé (où les hauts dirigeants apprennent des employés subalternes). Offrez des occasions d'apprentissage de manière uniforme à l'ensemble de l'équipe de cybersécurité, en veillant à soutenir les talents en milieu et en fin de carrière dans leur recherche de défis et de consolidation des compétences.

Faites de la formation en cybersécurité une priorité pour l'ensemble de l'entreprise. En ce qui concerne la cybersécurité, les employés d'une organisation constituent souvent le maillon le plus faible. Pour réduire les risques, accordez plus d'importance à la formation et à la sensibilisation relatives aux questions de cybersécurité pour tous les employés; vous aiderez ainsi les employés à protéger l'organisation et à se protéger eux-mêmes contre une violation de la sécurité. Assurez une sensibilisation et une formation qui leur permettent non seulement de mieux se prémunir contre les cyberrisques au travail, mais également d'améliorer la façon dont eux et les membres de leur famille interagissent avec l'information et la technologie à la maison.

Fidélisation

Faites de la fidélisation une priorité. Les organisations qui investissent dans des personnes qui cadrent avec leur proposition de valeur en matière de talents sont en meilleure position pour attirer et fidéliser les types de talents dont elles ont besoin pour demeurer compétitives. Il est toutefois important de reconnaître qu'il est impossible de retenir tout le monde; les organisations doivent donc être stratégiques. Repérez les talents très performants ou ayant un fort potentiel futur en fonction de leurs compétences en leadership, de leurs capacités difficiles à remplacer et de leur valeur en tant que modèles, puis faites un effort supplémentaire pour vous assurer de les fidéliser.

Mettez l'accent sur :

La génération millénaire. Il est particulièrement important d'attirer et de fidéliser les jeunes travailleurs, qui seront les piliers de vos futurs programmes de cybersécurité. Offrez des horaires de travail flexibles et des milieux de travail plus décontractés et situés à des emplacements convenant aux jeunes travailleurs. Les millénaux souhaitent généralement travailler pour des organisations sensibles aux enjeux qui leur tiennent à cœur, notamment les questions économiques, environnementales et sociales actuelles. Il est important d'investir dans des initiatives de responsabilité d'entreprise et de souligner l'importance sociétale, économique et commerciale de la fonction de cybersécurité.

Les professionnels en milieu et fin de carrière. Les millénaux sont réputés être à la recherche d'un travail intéressant et constructif, mais c'est le cas pour les talents de tous les échelons hiérarchiques et de tous les niveaux d'expérience. Si vous fidélisez des talents en milieu et en fin de carrière vous vous assurerez de conserver votre bagage d'expérience, vos capacités intellectuelles, vos investissements en formation et, dans bien des cas, votre bassin de relève. Prenez le temps d'interroger tous les employés pour vous assurer que vous respectez votre proposition de valeur en matière de talents, et intégrez les nouveaux besoins à votre plan.

Ouvrez votre portefeuille. Nous avons révélé que 30 % des dirigeants ont indiqué que leurs régimes de rémunération et d'incitation ne suivent pas le rythme du marché, ce qui en fait le principal défi du perfectionnement et de la fidélisation. Dans un domaine critique où les ressources sont insuffisantes, comme la cybersécurité, les salaires sont élevés et probablement supérieurs à ceux de postes comparables d'autres services.

Cela crée des tensions à l'interne, car les dirigeants tentent d'offrir des salaires concurrentiels sur le marché tout en respectant leurs structures de rémunération officielles et en préservant l'équité interne. Une certaine souplesse ou créativité sera nécessaire dans les programmes de rémunération des entreprises pour donner aux dirigeants les moyens d'attirer et de retenir les talents dans un contexte de rareté.

Autres tactiques à envisager :

- Améliorez la notoriété de votre marque et de votre proposition de valeur en matière de talents afin de mener la conversation plus loin que les simples questions de rémunération.
- Mettez en œuvre l'automatisation et les technologies cognitives pour réduire votre besoin d'expertise humaine.
- Payez pour la résolution de vos plus grands défis – lancez une initiative d'externalisation ouverte visant vos problèmes les plus difficiles et vos lacunes en matière d'innovation, et offrez des récompenses financières importantes pour leur résolution (de 20 000 $ à plus de 50 000 $, selon la complexité et la gravité du problème).

Départs

Ne brûlez pas les ponts. Dans un marché à forte demande, il est inévitable que certains membres de l'équipe choisissent de partir. Il est cependant important de les traiter avec respect; vous pourriez les recruter de nouveau dans l'avenir. Vous voulez également que vos anciens employés parlent favorablement de votre organisation et de votre marque en matière de talents lors de leurs activités d'échange des connaissances. Si votre organisation n'est pas en mesure de répondre aux besoins de certains professionnels, aidez-les à trouver ce qu'il leur faut à l'externe, et quand quelqu'un quitte votre organisation, tirez-en les enseignements nécessaires qui vous permettront de vous améliorer.

5 Conclusion

Réduire l'écart lié aux cyberrisques et permettre aux organisations de tirer pleinement parti des nouvelles technologies représentent un défi majeur de notre époque. Les technologies émergentes telles que l'automatisation, l'intelligence artificielle, l'apprentissage machine et l'analyse avancée peuvent compléter les efforts de cybersécurité traditionnels d'une organisation. Cependant, ces technologies n'élimineront pas la nécessité d'avoir recours à des experts humains – du moins, pas de sitôt.

Dans un avenir rapproché, les entreprises, les établissements d'enseignement et les gouvernements canadiens devront considérer la pénurie de cybertalents sous un angle humain et prendre des mesures audacieuses et délibérées pour surmonter les obstacles.

L'utilisation du cadre sur les cybertalents et des personnalités permet de réfléchir autrement aux compétences et aux rôles requis, ce qui aidera les organisations à éliminer les barrières délimitant les différents rôles et à définir les compétences et les capacités essentielles à leur réussite future; une stratégie qui renforcera notre atout concurrentiel et notre position de leader sur la scène mondiale.

Remerciements

Ce rapport a été préparé par Deloitte S.E.N.C.R.L./s.r.l., en partenariat avec la Toronto Financial Services Alliance (TFSA), qui est financée en partie par la province de l'Ontario. Nous aimerions remercier les représentants du secteur des services financiers et des établissements d'enseignement postsecondaire qui ont pris part à nos groupes de discussion ainsi que tous ceux qui ont participé aux entretiens et répondu à notre sondage. Les auteurs tiennent à souligner les contributions inestimables de l'équipe de la TFSA et du personnel de recherche et de rédaction de Deloitte.

Notes

[1] Kaplan, J. M., Bailey, T., Rezek, C., OHalloran, D., et Marcus, A. (2015). *Beyond cybersecurity: Protecting your digital business.* Hoboken, NJ: Wiley.

[2,11] Frost & Sullivan. (2017). *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk.* Accessible à l'adresse : https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf.

[3] Presses de l'Université Deloitte. (2017). *Augmented security: How cognitive technologies can address the cyber workforce shortage.* Accessible à l'adresse : https://www2.deloitte.com/content/dam/insights/us/articles/3992_Augmented-security/DUP_Augmented-security.pdf

[4] Statistique Canada (2017). *Portrait de la scolarité au Canada : recensement de la population de 2016.* Accessible à l'adresse : https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2017036-fra.htm

[5] Conseil des technologies de l'information et des communications. (Avril 2017). *La prochaine vague de talents : Naviguer le virage numérique - Perspectives 2021.* Accessible à l'adresse : https://www.ictc-ctic.ca/wp-content/uploads/2017/04/ICTC_Perspectives-2021.pdf

[6,9] Oltsik, J. (Novembre 2017). *The Life and Times of Cybersecurity Professionals.* Accessible à l'adresse : https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/surveyes/ESG-ISSA-Research-Report-Lif.pdf

[7] Ponemon Institute LLC. (Juin 2017). *2017 Cost of Data Breach Study: Global Overview.* Accessible à l'adresse : https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

[8] Frost & Sullivan. (2017). *The 2017 Global Information Security Workforce Study: Women in Cybersecurity.* Accessible à l'adresse : https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

[11] Statistique Canada. (Septembre 2016). *Scolarité au Canada : niveau de scolarité, domaine d'études et lieu des études.* Accessible à l'adresse : http://www12.statcan.gc.ca/nhs-enm/2011/as-sa/99-012-x/99-012-x2011001-fra.cfm

[12,13] Serene-Risc. (2015). *Canadian Cybersecurity Course Directory.* Accessible à l'adresse : https://www.serene-risc.ca/fichiers/downloads/1/Course-Directory_v2.pdf

[14] CyberNB. (2018). *Opportunities NB and The Department of Education and Early Childhood Development on Cybersecurity Education and Digital Literacy.* Accessible à l'adresse : https://cybernb.ca/wp-content/uploads/2017/09/MOU_ONB_EECD_CYBERSECURITY.EDUCATION_AND_DIGITAL.LITTERACY_EN.pdf

[15] Ministère des Finances. (2018). *Plan axé sur le mieux-être et l'avenir.* Accessible à l'adresse : http://budget.ontario.ca/fr/2018/chapter-2.html

[16] Emploi et Développement social Canada.(Septembre 2017). *Programme d'apprentissage intégré en milieu de travail pour étudiants.* Extrait de l'adresse suivante : https://www.cewilcanada.ca/_Library/SWILP/CAFCE_ESDC_Webinar_Slides.pdf

[17] Ministère des Finances. (2018). *Plan axé sur le mieux-être et l'avenir.* Accessible à l'adresse : http://budget.ontario.ca/fr/2018/chapter-2.html

[18] Newhouse, W., Keith, S., Scribner, B., & Witte, G. (Août 2017). *NICE Cybersecurity Workforce Framework.* Accessible à l'adresse : https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[19] Banque Royale du Canada. (Janvier 2018). *RBC ouvrira un laboratoire de cybersécurité et financera de nouvelles recherches à l'Université de Waterloo.* Accessible à l'adresse : http://www.rbc.com/nouvelles/news/2018/20180129-cybersecurity-waterloo.html

[20] Université de la Colombie-Britannique. (Mars 2017). *Scotiabank funds $2-million cybersecurity and financial data initiative at UBC.* Accessible à l'adresse : https://science.ubc.ca/news/scotiabank-funds-2-million-cybersecurity-and-financial-data-initiative-ubc

[21] Sun Life Financial. (2018). Rotational Leadership Development Program. Accessible à l'adresse : http://www.sunlife.com/us/About+us/Careers/Student+and+new+graduate+programs/ch.Rotational+Leadership+Development+Program.mobile?vgnLocale=en_CA

Personnes-ressources

Marc MacKinnon

Leader national
Stratégies liées aux cyberrisques
mmackinnon@deloitte.ca

Steve Rampado

Associé, Conseils en
gestion des risques
srampado@deloitte.ca

Sashya D'Souza

TFSA
Vice-présidente principale
Iniatives en matière de talents
sdsouza@tfsa.ca

Julie Bryski

TFSA
Directrice,
Iniatives en matière de talents
jbryski@tfsa.ca

À propos de la Toronto Financial Services Alliance

La TFSA est un partenariat public-privé entre trois niveaux de gouvernement, le secteur des services financiers et les universités. La mission de la TFSA est de mener une action collective qui stimule la compétitivité et la croissance du secteur financier de Toronto et établit son importance en tant que centre financier international de premier plan. Pour obtenir plus d'information, veuillez visiter tfsa.ca.

Deloitte.

www.deloitte.ca

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans de nombreux secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500MD par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Pour en apprendre davantage sur la façon dont les quelque 264 000 professionnels de Deloitte ont une influence marquante – y compris les 9 400 professionnels au Canada – veuillez nous suivre sur LinkedIn, Twitter ou Facebook.

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 18-5551M