ÉCOLE NATIONALE D'ADMINISTRATION PUBLIQUE

RAPPORT DE STAGE EFFECTUÉ À L'INSTITUT NATIONAL DES MINES

PRÉSENTÉ

AU BUREAU DES STAGES

COMME EXIGENCE PARTIELLE À LA RÉALISATION DE L'ACTIVITÉ D'INTÉGRATION

ENP7969-S – STAGE

PAR

NICHOLAS THÉROUX

MATRICULE : E0322292

DÉCEMBRE 2020

Table des matières

Remerciements 2
Liste des tableaux 3
Liste des figures 4
Liste des sigles 5
Lexique 6
Résumé 7
Introduction 9
Description de l'organisation et du mandat 12
Recension des écrits - La cybersécurité dans le secteur minier à l'ère de la 4e révolution industrielle 14
Méthodologie de recherche 28
Résultats 32
Discussions, recommandations et limites 49
Conclusion 53
Bibliographie 55
Annexe I 60

Remerciements

En premier lieu, je tiens à remercier mes conseillers académiques, monsieur Éric Charest et madame Nancy Brassard. C'est grâce à leur soutien et à leur expérience que ce rapport de stage prend forme aujourd'hui. Je remercie également l'ensemble du personnel de l'École nationale d'administration publique, dont l'équipe du bureau des stages, pour son professionnalisme et sa rigueur. Enfin, les membres du personnel de l'Institut national des mines ont été toujours présents pour moi durant mon stage et je les en remercie sincèrement.

Je remercie également du fond du cœur mon camarade de classe Claude Pelletier qui a su m'encourager dans les moments difficiles et faire de l'expérience universitaire une période encore plus mémorable grâce à sa bonne humeur contagieuse.

Finalement, je ne saurais passer sous silence le soutien de ma famille, de mes amis et de ma conjointe tout au long de ce processus unique que fut cette maîtrise en administration publique. Je tiens particulièrement à remercier mes parents Chantal et Richard pour leurs encouragements constants, ma grand-mère Simone pour sa fierté et ma chère Roxanne pour son soutien inconditionnel.

Liste des tableaux

Tableau 1 - Cadre synthèse inventoriant et catégorisant les quatre types d'acteurs à l'origine des cyberrisques…… 19

Tableau 2 - Conséquences possibles d'une cyberattaque affectant les infrastructures opérationnelles d'une entreprise minière…….. 22

Tableau 3 - La famille de compétences numériques « Protéger » selon « Le cadre de référence des compétences à l'ère du numérique dans le secteur minier »……... 27

Tableau 4 - Établissements d'enseignement interrogés ……..…… 30

Tableau 5 - Fonction occupée par les personnes répondantes dans les établissements d'enseignement……. 31

Tableau 6 - Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques…….. 33

Tableau 7 - Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations…….……. 35

Tableau 8 - Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à la gestion des risques numériques ……..… 37

Tableau 9 - Instauration d'autres activités ayant pour but la sensibilisation à toute notion relative à la cybersécurité……..…… 39

Tableau 10 - Probabilité d'instauration d'activités pédagogiques sensibilisant à la cybersécurité au cours des deux prochaines années……...….... 41

Tableau 11 - Perception du niveau d'importance que le secteur minier doit accorder à la cybersécurité dans ses activités……. 41

Tableau 12 - Perception de la nécessité de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier……. 42

Tableau 13 - Perception du niveau de compétence en cybersécurité devant être possédée pour occuper des postes dans le secteur minier……..... 44

Tableau 14 - Niveau d'accord avec l'idée d'inclure l'acquisition d'une compétence reliée à la cybersécurité dans le devis ministériel…….……. 46

Liste des figures

Figure 1 - Les six familles de compétences numériques du « Cadre de référence des compétences à l'ère du numérique dans le secteur minier »…….…… 26

Figure 2 - Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques……...… 34

Figure 3 - Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations.……..…… 36

Figure 4 -Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à la gestion des risques numériques…..……. 38

Figure 5 - Perception, par ordre d'enseignement, de la nécessité de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier…… 43

Figure 6 - Perception, par ordre d'enseignement, du niveau de compétence en cybersécurité devant être possédé pour occuper des postes dans le secteur minier…… 45

Figure 7 - Niveau d'accord, par ordre d'enseignement, avec l'idée d'inclure l'acquisition d'une compétence reliée à la cybersécurité dans le devis ministériel…….…... 47

Liste des sigles

CSMO Mines : Comité sectoriel de la main-d'œuvre de l'industrie des mines

DEC : Diplôme d'études collégiales

DEP : Diplôme d'études professionnelles

INMQ : Institut national des mines du Québec

Lexique

Cyberattaque

Ensemble coordonné d'actions malveillantes conduites par l'intermédiaire du cyberespace, qui visent à endommager, à forcer ou à détourner un réseau ou un système informatique afin de commettre un acte préjudiciable[1].

Cyberespace

Espace virtuel constitué par l'interconnexion mondiale des systèmes informatiques, des réseaux de télécommunication et des infrastructures de technologies de l'information, qui permet l'échange d'informations entre utilisateurs individuels ou collectifs[1].

Cyberhygiène

Ensemble des règles à observer et des pratiques récurrentes qui sont associées à la sécurité d'un système d'information[1].

Cyberprotection

Ensemble des moyens, techniques ou juridiques, qui contribuent à assurer la cybersécurité[1].

Cyberrisque

Ensemble de risques liés à l'utilisation des technologies de l'information[1].

Cybersécurité

L'approche et les actions associées aux processus de gestion des risques de sécurité suivis par les organisations et les États pour protéger la confidentialité, l'intégrité et la disponibilité des données et des actifs utilisés dans le cyberespace. Le concept comprend les lignes directrices, les politiques […], les technologies, les outils et les formations utilisés pour fournir la meilleure protection à l'état du cyberenvironnement et à ses utilisateurs (*traduction libre*)[2].

Internet des objets

L'Internet des objets (IoT, Internet of things) caractérise les objets physiques connectés, ayant leur propre identité numérique et étant capables de communiquer les uns avec les autres par Internet ou d'autres réseaux de connexion[3].

---

[1] Définition de la *Politique gouvernementale de cybersécurité* (Secrétariat du Conseil du trésor, 2020, p. 2).
[2] Définition provenant de l'article *Towards a More Representative Definition of Cyber Security* (Schatz et al., 2017, p. 66).
[3] Définition du ministère de l'Économie et de l'Innovation (MEI, 2019).

Résumé

Depuis 2018, la veille informationnelle hebdomadaire réalisée par l'Institut national des mines témoigne de l'importance majeure qu'occupent les enjeux reliés à la cybersécurité pour l'industrie minière dans le contexte où celle-ci intensifie sa transformation numérique. La numérisation accrue des outils de travail ainsi que la connectivité croissante des équipements industriels constituent autant d'éléments faisant en sorte que l'acquisition de compétences en cybersécurité représente un incontournable pour la main-d'œuvre évoluant dans le secteur minier du 21e siècle. Les objectifs recherchés par ce rapport sont à la fois de documenter la place accordée à la cybersécurité dans les programmes de formation minière les plus en demande au Québec, mais également d'en apprendre davantage sur la perception des établissements d'enseignement offrant ces formations à l'égard de la cybersécurité en formation minière.

Les résultats recueillis démontrent que la sensibilisation des personnes apprenantes en formation minière aux trois actions-clés en cybersécurité requises à l'ère du numérique dans les mines demeure limitée. En effet, aucune des trois actions-clés ne fait l'objet d'une sensibilisation dans une majorité de programmes de formation professionnelle et collégiale. Toutefois, l'ensemble des personnes répondantes des programmes de formation sondés jugent que la cybersécurité est importante dans le secteur minier, c'est pourquoi la plupart estiment qu'ils instaureront probablement au moins une activité pédagogique visant la sensibilisation à la cybersécurité d'ici 2022. Les mêmes personnes répondantes considèrent que ce sont principalement des compétences en cybersécurité d'un niveau de base et d'un niveau intermédiaire qui sont nécessaires pour travailler dans le secteur minier actuel. La majorité des personnes répondantes indiquent donc, par conséquent, être favorables à l'idée d'inclure l'acquisition d'une compétence en cybersécurité dans les devis ministériels encadrant les programmes de formation minière.

Les données colligées dans le cadre de cette recherche illustrent le fait que les personnes répondantes des établissements d'enseignement du Québec offrant de la formation minière

considèrent qu'il est important que les personnes apprenantes fassent l'acquisition de compétences en cybersécurité. Cependant, il appert que les initiatives déployées à cet égard sont plutôt restreintes et elles sont de surcroît variables d'un programme de formation à l'autre et même d'un établissement d'enseignement à l'autre.

Introduction

À l'ère de l'industrie 4.0, les activités de l'ensemble du processus de développement minéral sont transformées. En effet, l'émergence de la mine intelligente, dans laquelle l'intégration sans cesse croissante des données numériques dans la prise de décision automatisée ou humaine contribue à rendre les opérations minières de plus en plus agiles, bouleverse les processus de travail préexistants (Institut national des mines, 2018b). Pour évoluer de manière optimale dans ce contexte professionnel en constante transformation, l'Institut national des mines soutient que la main-d'œuvre du secteur minier doit développer ses compétences numériques, et ce, afin d'améliorer l'adéquation entre son savoir-agir et les compétences requises sur le marché du travail d'aujourd'hui et de demain (Institut national des mines, 2018b). Ce constat est partagé par le ministère de l'Éducation et le ministère de l'Enseignement supérieur qui stipulent, au sein du *Cadre de référence de la compétence numérique,* que « la compétence numérique est intimement liée au développement professionnel de tous les travailleurs et travailleuses du 21e siècle » (Ministère de l'Éducation et de l'Enseignement supérieur, 2019, p. 7). Pour le ministère, cette « compétence numérique » se décline en douze dimensions, chacune de ces dimensions étant constituée de plusieurs éléments, c'est-à-dire des habiletés associées à la maîtrise de la dimension ciblée (Ministère de l'Éducation et de l'Enseignement supérieur, 2019, p. 11). Le *Cadre de référence de la compétence numérique* a permis au ministère d'identifier que la dimension intitulée *Développer et mobiliser ses habiletés technologiques* représente l'une « des dimensions centrales autour desquelles s'articulent les autres dimensions » (Ministère de l'Éducation et de l'Enseignement supérieur, 2019, p. 9-14). Au cœur des éléments nécessaires à la maîtrise de cette dimension jugée centrale figure l'aptitude à « sécuriser des données personnelles à l'aide des ressources appropriées, notamment en considérant les risques liés à l'utilisation du numérique » (Ministère de l'Éducation et de l'Enseignement supérieur, 2019, p. 14).

Cette importance qu'accorde le *Cadre de référence de la compétence numérique* à la possession par la main-d'œuvre du 21e siècle de compétences en matière de cybersécurité

concorde avec les constats réalisés par l'Institut national des mines. En effet, depuis 2018, la veille informationnelle réalisée de manière hebdomadaire par l'Institut national des mines a permis de repérer que la question du cyberrisque constitue un enjeu prioritaire pour un nombre croissant d'acteurs du secteur minier (Institut national des mines, 2018a). Depuis ce moment, cette tendance ne s'est pas démentie puisque la veille informationnelle de l'Institut continue de démontrer jusqu'à ce jour que la cybersécurité représente l'une des priorités majeures de l'industrie minière contemporaine. Ce souci particulier envers la cybersécurité découle notamment du fait qu'avec le développement rapide de l'Internet des objets au sein de l'industrie minière, le risque de cyberattaque ne cesse de s'accroître puisque la surface d'attaque, c'est-à-dire la quantité de cibles potentielles, s'élargit au même rythme que les divers équipements opérationnels deviennent de plus en plus connectés (Ernst & Young et associés, 2018). Ce souci croissant des entreprises du secteur minier envers leur cybersécurité a été documenté en 2020 par la société de télécommunication Inmarsat dans son rapport intitulé *The Rise of IOT in Mining*. En se basant sur un échantillon de 200 entreprises minières actives aux quatre coins de la planète, Inmarsat a en effet découvert que les sociétés minières sont tout à fait conscientes des dommages importants pouvant résulter d'une cyberattaque, et de l'éventail grandissant de menaces auxquelles elles font face à mesure qu'elles introduisent une quantité croissante d'objets connectés à Internet dans leurs opérations (Inmarsat, 2020). Dans un rapport de 2017, la firme de conseil Willis Towers Watson soulignait de se son côté que la vaste majorité des entreprises investissant afin d'améliorer leurs infrastructures de cybersécurité se considèrent malgré tout vulnérables face aux cyberattaques (Willis Towers Watson, 2017). Ce paradoxe découle du fait que même les infrastructures technologiques les plus sophistiquées ne sont pleinement efficaces que si elles sont utilisées par une main-d'œuvre pleinement qualifiée. Mais la main-d'œuvre minière québécoise reçoit-elle la formation initiale adéquate afin de faire face efficacement à cet enjeu qui est de plus en plus incontournable à l'ère de la quatrième révolution industrielle?

Objectifs du rapport de stage

Ce rapport entend analyser la place accordée à la cybersécurité dans la formation minière dispensée dans les établissements d'enseignement du Québec ainsi que la perception de ces

mêmes établissements à l'égard de la cybersécurité. De plus, grâce à la rédaction d'une recension des écrits portant sur l'importance de la cybersécurité dans le secteur minier à l'ère de l'industrie 4.0, ce rapport permet de réfléchir sur la place de la cybersécurité dans les cursus scolaires menant à l'exercice d'un métier ou d'une profession du secteur minier.

Plan sommaire du rapport de stage

Ce rapport de stage est articulé en six chapitres distincts. Tout d'abord, le premier chapitre décrit le mandat du stagiaire et le contexte organisationnel dans lequel celui-ci a réalisé ce rapport de stage. Le deuxième chapitre présente une recension des écrits détaillant l'importance des compétences en cybersécurité dans l'industrie minière à l'ère de la quatrième révolution industrielle et de la mine intelligente. Le troisième chapitre détaille la méthodologie utilisée pour collecter les données nécessaires à l'élaboration de cette recherche. Par la suite, le quatrième chapitre est l'occasion de présenter un état de la situation concernant la sensibilisation aux actions-clés relatives à la cybersécurité dans la formation minière québécoise. De plus, la perception des établissements d'enseignement du Québec offrant de la formation minière à l'égard de la cybersécurité dans les cursus menant à l'exercice d'un métier ou d'une profession du secteur minier est également étudiée. Le cinquième chapitre permet d'analyser l'état de situation présenté au troisième chapitre. Cette démarche fait ressortir les éléments marquants ainsi que la corrélation entre les résultats obtenus et la littérature scientifique disponible sur le sujet. Finalement, le sixième chapitre vise à faire émerger des pistes de recherche susceptibles de favoriser le développement de compétences en cybersécurité dans la formation minière québécoise.

Description de l'organisation et du mandat

Présentation du mandat

Le mandat que l'étudiant s'est vu attribuer par le mandant est la réalisation d'un rapport de recherche portant sur la cybersécurité en formation minière au Québec, un mandat répondant aux objectifs poursuivis par l'Institut national des mines. L'objectif recherché par le mandant était l'obtention d'un portrait des initiatives pédagogiques relatives à la cybersécurité en place dans les établissements d'enseignement du Québec offrant de la formation minière.

Par la réalisation de ce rapport, l'organisme hôte vise l'atteinte de l'un des objectifs énoncés au sein de sa planification stratégique. En effet, le deuxième objectif de la planification stratégique 2018-2023 de l'Institut national des mines stipule que l'organisme doit annuellement publier un rapport faisant l'analyse des « tendances en innovation susceptibles d'avoir un impact sur la formation minière au Québec » (Institut national des mines, 2020, p. 17).

Le mandant n'a pas mentionné au stagiaire une ampleur spécifique en ce qui concerne la taille du document. Le mandant a toutefois stipulé que le document devait être de calibre universitaire et donc, reposer sur l'approche de la recherche scientifique. La réalisation d'un processus de recherche classique incluant une problématisation, la réalisation d'une recension des écrits, l'élaboration d'une méthodologie, la collecte des données, la présentation des données et l'analyse des données était donc attendu du stagiaire. Les tâches confiées au stagiaire ont donc été d'élaborer la structure du rapport ainsi que sa méthodologie, de réaliser la collecte de données et de rédiger le rapport. La conceptualisation de la structure et de la méthodologie du rapport se sont faites à l'hiver 2020, tandis que la collecte de données a eu lieu au printemps et à l'été 2020. La rédaction du rapport s'est quant à elle déroulée à l'automne 2020. Le mandat, et donc les tâches s'y rattachant, a été clairement détaillé au stagiaire dès le début du stage. Le mandat n'a pas été modifié au cours du stage, car l'objectif établi initialement est resté le même tout au long du processus de stage.

La mission de l'organisation et comment le mandat se situe dans l'organisation

La mission de l'Institut national des mines est de conseiller le ministre de l'Éducation, ainsi que le ministre de l'Enseignement supérieur, en matière de formation dans le secteur minier (Loi sur l'Institut national des mines, 2013). Bien que l'Institut conseille les deux ministres, c'est le ministre de l'Éducation, et non lui de l'Enseignement supérieur, qui est le ministre duquel relève l'Institut national des mines. Pour mener à bien son mandat, l'Institut peut notamment réaliser des études, des projets-pilotes, des partenariats avec des acteurs du secteur minier et même des collaborations internationales avec des gouvernements étrangers (Loi sur l'Institut national des mines, 2013). Cette organisation compte sur des ressources humaines limitées afin de réaliser ses activités puisque seulement sept personnes sont à l'emploi de l'organisme. La petite taille de l'organisation a pour effet de faire en sorte qu'il n'existe pas de directions ou de services officiellement constitués à l'Institut national des mines. Toutefois, les employés sont divisés de manière informelle en trois « services » distincts que sont : l'administration, les communications et les projets de recherche. Durant le stage, nous avons travaillé au sein du « service » des projets de recherche. Le rôle de ce « service » est de réaliser ou de superviser les projets de recherche que mène l'Institut afin de documenter l'évolution des besoins de formation minière au Québec. Puisque l'Institut est un organisme-conseil qui ne livre pas de services à la population, mais qui aide plutôt le gouvernement du Québec dans la mise en œuvre d'une formation minière adaptée à la réalité du 21^{e} siècle, les projets de recherche réalisés par ce « service » sont au centre de ses activités, car ce sont ceux-ci qui permettent d'élaborer les recommandations qui seront formulées à l'intention des ministres.

Recension des écrits - La cybersécurité dans le secteur minier à l'ère de la 4e révolution industrielle

Industrie minière et révolution industrielle 4.0 : l'émergence de la mine intelligente

À l'ère de la quatrième révolution industrielle, tous les secteurs industriels sont appelés à évoluer sous l'influence d'innovations technologiques transformant radicalement les façons de faire préexistantes. Le secteur minier n'échappe pas à ces processus de transformation puisque les diverses technologies propres à l'industrie 4.0 y sont d'ores et déjà mises à profit afin d'optimiser les activités et les processus. Il est notamment possible de citer à titre d'exemple l'automatisation de certaines activités, telle l'opération de véhicules de manière autonome ou télécommandée depuis un centre de contrôle pouvant être situé à des milliers de kilomètres du complexe minier où se déroule l'extraction du minerai.

Mais qu'est-ce que la quatrième révolution industrielle, communément appelée « l'industrie 4.0 »? Selon le ministère de l'Économie et de l'Innovation, « l'industrie 4.0 […] se caractérise fondamentalement par une automatisation intelligente et par une intégration de nouvelles technologies à la chaîne de valeur de l'entreprise » (Ministère de l'Économie et de l'Innovation, 2018). Un élément central de cette révolution industrielle se trouve dans l'interconnectivité des systèmes, une interconnectivité qui permet de mettre en commun en temps réel les données captées, puis de mobiliser divers algorithmes pour extraire des données l'information nécessaire à une prise de décision optimale (Institut national des mines, 2018b). C'est donc ce qui permet d'affirmer que « le caractère proprement révolutionnaire de l'industrie 4.0 […] provient […] de l'ajout d'une brique technologique transversale qui interconnecte et synchronise les différents systèmes de production les uns avec les autres, quelle que soit leur localisation géographique » (Kohler & Weisz, 2016).

L'impact exercé par cette révolution industrielle sur l'industrie minière est incommensurable, et ce, d'autant plus que des innovations alimentant cette transformation ne cessent d'émerger. Au stade où se situe actuellement la quatrième révolution industrielle, l'Institut national des mines estime que le concept de « mine intelligente » est celui qui permet le mieux de définir

l'impact de l'industrie 4.0 sur le secteur minier. Selon ce concept, les mines qui procèdent à leur transition vers l'industrie 4.0 deviennent « intelligente », c'est-à-dire qu'un « processus d'acquisition de données par les équipements et les individus » y est implanté et que l'information ainsi captée est mise au service d'un processus de prise de décisions optimisé (Institut national des mines, 2018b, p. 17).

Cependant, pour que le concept de « mine intelligente » passe de la théorie à la réalité, les données doivent non seulement d'abord être captées, mais elles doivent ensuite être enregistrées, traitées, analysées, communiquées et protégées (Institut national des mines, 2018b). Cela signifie donc que « la connectivité des données et des objets est la composante déterminante de l'industrie 4.0 » (Ministère de l'Économie et de l'Innovation, 2016).

Les données et la connectivité : les éléments centraux de la quatrième révolution industrielle dans le secteur minier

Les données et la connectivité sont donc au cœur de la quatrième révolution industrielle puisque la possibilité de transmettre les données collectées constitue un élément incontournable dans la mise en place de la mine intelligente. Cette transmission des données captées est désormais rendue possible grâce à l'essor au cours des dernières années de l'Internet des objets. En effet, en concrétisant la convergence entre les technologies de l'information et les technologies opérationnelles, l'Internet des objets permet la connexion des objets à Internet ou à d'autres réseaux de connexion. Les objets connectés, qui se voient également implanter des appareils tels des capteurs et des puces électroniques, deviennent ainsi à même de transmettre une variété de données numériques sur Internet ou d'autres réseaux de connexion (Forum économique mondial, 2017).

Cependant, pour que les données captées puissent être intégrées en temps réel dans les processus de prise de décisions et ainsi être utilisées à leur plein potentiel, un complexe minier doit pouvoir compter sur une connectivité particulièrement fiable et de haut débit. Par le passé, cette connectivité a constitué un frein important à l'automatisation des activités minières, que ce soit en raison de l'éloignement des sites miniers des centres urbains ou encore en raison des difficultés liées à l'implantation d'une connectivité fiable dans les

galeries des mines souterraines. Aujourd'hui, bien que ces réalités continuent de poser des défis en ce qui a trait à la connectivité des complexes miniers, les nouvelles avancées technologiques permettent néanmoins aux entreprises minières d'entreprendre le tournant 4.0. En effet, dans sa plus récente étude portant sur l'Internet des objets dans le secteur minier, la société Inmarsat a constaté que parmi son échantillon de 200 entreprises minières réparties aux quatre coins de la planète, 67 % d'entre elles avaient d'ores et déjà complété au moins 1 projet reposant sur l'Internet des objets (Inmarsat, 2020). Toujours selon Inmarsat, cette intégration de l'Internet des objets dans les activités de production minérale est notamment rendue possible grâce au développement de l'Internet satellitaire ainsi qu'à l'implantation accrue de réseaux LTE sur les sites miniers (Inmarsat, 2020).

Les avantages reliés à l'implantation de technologies associées à l'Internet des objets dans le secteur minier sont nombreux (Inmarsat, 2020). En effet, l'implantation de capteurs sur les multiples équipements déployés dans un complexe minier permet de créer un véritable réseau d'appareils connectés. Lorsque ce réseau est interconnecté avec le système informatique, l'entreprise a accès à une quantité phénoménale de données en temps réel. Ces données peuvent alors être agrégées à l'aide d'algorithmes, de logiciels ou même de solutions reposant sur l'intelligence artificielle afin de dégager une vision holistique de la situation et des activités en cours dans une mine (Austmine, 2018). Mais cette interconnexion entre les systèmes opérationnels et les systèmes informatiques permet également de contrôler et de surveiller à distance des équipements automatisés pouvant réaliser des tâches aussi diversifiées que du forage, du dynamitage, de l'extraction ou du transport de minerai (Austmine, 2018).

Les investissements de plus en plus importants que prévoit réaliser l'industrie minière pour déployer l'Internet des objets dans ses opérations témoignent d'ailleurs de la place centrale qu'occupe cette technologie dans la vision stratégique à long terme développée par les entreprises minières pour augmenter la productivité de leurs opérations, diminuer leurs coûts d'exploitation et améliorer la santé et la sécurité au travail de leur main-d'œuvre. En effet, à l'échelle mondiale, les entreprises minières ont consacré en moyenne 3,9 % de leur budget dédié aux technologies de l'information à des projets basés sur l'Internet des objets au cours

des trois années ayant précédé 2020 et cette proportion augmentera en moyenne à 7,6 % pour les trois années qui suivront 2020 (Inmarsat, 2020). La connexion d'une proportion croissante de matériel mobile et fixe à Internet soulève cependant des enjeux importants en matière de cybersécurité.

L'enjeu de la cybersécurité dans un contexte de connectivité accrue et de production croissante de données

Dans une étude portant sur la cybersécurité dans l'industrie minière, le cabinet de conseil Ernst & Young et associées stipule que le degré élevé de connectivité caractérisant désormais les technologies opérationnelles déployées dans les complexes miniers nécessite l'émergence d'une nouvelle façon de concevoir la cybersécurité dans le secteur des mines (Ernst & Young et associés, 2018). En effet, dans les mines dites « traditionnelles », dont les activités industrielles reposaient sur des technologies opérationnelles peu connectées, le cyberrisque auquel faisait face les entreprises minières était restreint, car une faible quantité d'équipements étaient connectés et parmi l'équipement connecté, rare était la connectivité à des réseaux externes. Or, le développement rapide des technologies associées à l'Internet des objets et l'automatisation croissante des sites miniers ont changé la donne en augmentant considérablement les cyberrisques qu'encoure un complexe minier (Ernst & Young et associés, 2018). L'interconnexion entre les systèmes et l'intégration entre les technologies de l'information (TI) et les technologies opérationnelles (TO) augmente donc aujourd'hui considérablement l'ampleur des dégâts qu'un piratage est susceptible de causer lors d'une cyberattaque fructueuse. En effet, l'intégration TI/TO permet dans certaines circonstances aux pirates qui réussissent à accéder à un réseau informatique de pousser plus loin leur intrusion et de s'attaquer au système opérationnel qui y est interrelié, compromettant ainsi l'intégrité des équipements, notamment ceux de surveillance ou de contrôle, qui servent à mener à bien les diverses activités industrielles du secteur minier (Austmine, 2018).

La prise de conscience du cyberrisque

Cette menace croissante fait en sorte que la mise en place d'une cybersécurité efficace constitue désormais une priorité pour de nombreuses sociétés du secteur minier, comme en

témoigne la progression du niveau d'inquiétude envers les cyberrisques parmi les dix plus grandes sociétés minières du monde (Marsh, 2018). En effet, en 2007, seulement une société minière parmi les dix sociétés ayant les plus importantes capitalisations boursières de la planète considérait les cyberrisques comme l'une des principales menaces à l'atteinte de ses objectifs. Or, depuis 2015, l'ensemble de ces dix entreprises classent les cyberrisques comme l'une des plus importantes menaces à l'atteinte de leurs objectifs. D'ailleurs, les cyberrisques représentent non seulement une préoccupation pour les très grandes entreprises minières, mais également pour la majorité des autres sociétés actives dans ce secteur puisqu'à l'échelle mondiale 57 % des dirigeants d'entreprises minières mentionnent avoir « des inquiétudes » en ce qui concerne la cybersécurité de leur organisation (PwC, 2020b). De cette prise de conscience quant à l'ampleur de la menace représentée par les cyberrisques, découle une volonté d'améliorer la résilience organisationnelle en matière de cybersécurité. Cette volonté est notamment illustrée par les investissements réalisés par l'industrie minière en matière de cyberprotection. En effet, selon une enquête menée à l'échelle mondiale, les sociétés minières prévoient doubler la proportion de leur budget informatique alloué à la cybersécurité entre 2020 et 2023, cette proportion étant appelée à passer de 4,2 % pour les trois années qui précédent 2020 à 8,4 % pour les trois années qui suivent 2020 (Inmarsat, 2020).

Mais cette préoccupation envers les enjeux reliés à la cybersécurité n'est pas propre qu'au secteur minier puisque de nombreuses études révèlent que les entreprises actives dans l'ensemble des secteurs d'activités s'intéressent de manière croissante aux cyberrisques et à la manière de les contrer. En effet, selon une enquête menée auprès de 1 500 dirigeants d'entreprises provenant de secteurs d'activités diversifiés et de tous les continents, 79 % des organisations considéraient en 2019 que les cyberrisques représentaient l'une des cinq principales préoccupations de leur organisation alors que cette proportion ne s'élevait qu'à 62 % en 2017 (Marsh et Microsoft, 2019). Ce souci à l'égard de la cybersécurité est d'ailleurs particulièrement important en Amérique du Nord comme le révèle une enquête menée en 2019 auprès de plus de 3 500 présidents-directeurs généraux de grandes entreprises réparties partout dans le monde. Selon cette étude, c'est en Amérique du Nord que les présidents-directeurs généraux craignent le plus les cyberrisques, ceux-ci étant d'ailleurs considérés

comme la plus grande menace qui pèse sur les perspectives de croissance économique (PwC, 2020a). Au Canada, la société d'informatique CDW Canada souligne dans son étude intitulée *Cyber Resilience: An Evolving Perspective* que les entreprises canadiennes « commencent à prendre la [cyber]sécurité plus au sérieux », et ce, notamment en raison du nombre important de cyberattaques subies annuellement et des coûts importants qui sont engendrés lorsque l'une des cyberattaques porte ses fruits et que des données personnelles et/ou corporatives sont compromises (CDW Canada, 2020).

L'origine de la menace

L'identité des individus ou des groupes à l'origine du cyberrisque qui se pose à l'endroit de l'industrie minière est hétérogène et leurs motivations le sont tout autant. L'identité et les motivations de ces individus et de ces groupes seront présentées dans les pages suivantes. Le **tableau 1** synthétise les quatre grands groupes d'acteurs qui sont à même de représenter un cyberrisque pour les organisations.

Tableau 1 – Cadre synthèse inventoriant et catégorisant les quatre types d'acteurs à l'origine des cyberrisques

	Interne	**Externe**
Malveillant	Acteur malveillant interne	Acteur malveillant externe
Involontaire	Acteur involontaire interne	Acteur involontaire externe

Source : RSA Security (2016).

Selon la firme Deloitte, ce sont des acteurs malveillants externes qu'émanent principalement les cyberrisques qui pèsent sur l'industrie minière. En effet, les États, les activistes politiques et les entreprises rivales représentent les trois acteurs identifiés comme étant particulièrement susceptibles de constituer une menace pour la cybersécurité des entreprises du secteur minier (Deloitte, 2018). En ce qui a trait aux États, ils peuvent retirer de nombreux gains de la perpétration de cyberattaques à l'encontre d'une société active dans le secteur des mines,

mais les deux principaux sont les suivants. D'abord, grâce au vol de données, un État peut se procurer de la propriété intellectuelle pouvant conférer un avantage concurrentiel à ses propres activités minières. De plus, la réalisation d'une cyberattaque affectant les technologies opérationnelles d'un site minier est susceptible d'endommager ou de détruire des infrastructures minières d'une importance critique pour un État rival (Austmine, 2018). Les États disposant en général de moyens techniques et financiers importants, le cyberrisque qu'ils sont à même de faire peser sur une organisation est d'autant plus à prendre en considération.

Les activistes politiques représentent également une nébuleuse d'acteurs pouvant potentiellement faire peser un cyberrisque sur les entreprises du secteur minier. Les objectifs que ceux-ci peuvent rechercher par l'entremise de leurs cyberattaques varient du vol de données corporatives pouvant être utilisées à des fins politiques jusqu'au sabotage d'équipements opérationnels en vue de ralentir ou d'arrêter la production pour des motifs sociopolitiques ou environnementaux (Austmine, 2018).

Les entreprises concurrentes sont également identifiées comme une menace potentielle à prendre en compte en raison des avantages stratégiques que peut retirer une entreprise de la perpétration d'une cyberattaque à l'encontre d'une autre entreprise. En effet, au-delà du sabotage d'équipement connecté visant à amoindrir la productivité d'une société rivale, c'est plutôt le vol de données corporatives qui semblent constituer la menace la plus concrète en matière de cyberattaque menée par une entreprise contre une autre. Les données volées à une société concurrente peuvent non seulement servir à obtenir des informations sur la stratégie d'affaires d'une entreprise rivale qui pourront être utilisées pour mieux concurrencer celle-ci, mais elles sont également susceptibles d'être d'une grande utilité en prévision de négociations entre sociétés (Austmine, 2018; Deloitte, 2018).

Par ailleurs, la recension des écrits a également permis de repérer un autre groupe d'acteurs malveillants externes. Il s'agit des cybercriminels motivés par les possibilités de réaliser des gains financiers par l'entremise du vol de données et de l'extorsion (Austmine, 2018). En effet, ces individus pouvant agir seuls ou en groupes n'épargnent aucun secteur d'activités comme en témoigne la vague de cyberattaques ayant ciblé plusieurs entreprises minières

canadiennes entre 2013 et 2016 et s'étant soldées par le vol d'une quantité importante de données personnelles et corporatives sensibles (Jenish, 2018).

Bien entendu, les acteurs malveillants externes ne représentent pas l'entièreté des individus ou des groupes faisant peser un cyberrisque sur l'industrie minière. Parmi la multitude de sources de danger potentiel pour la cybersécurité des sociétés minières, la revue de littérature réalisée dans le cadre de ce rapport a permis d'identifier que les acteurs internes représentent également une menace potentielle devant être considérée par les entreprises du secteur minier (Deloitte, 2018). En effet, des employées ou des employés à l'emploi d'une société minière, ou encore des membres du personnel d'un sous-traitant engagé par une entreprise minière, sont susceptibles de faire peser un cyberrisque important sur une organisation. Que les acteurs internes agissent de manière involontaire ou qu'ils soient animés d'intentions malveillantes, leur positionnement au sein de l'organisation leur permet parfois d'avoir un accès privilégié à certaines infrastructures physiques ou numériques critiques à la cyberprotection de l'organisation (RSA Security, 2016). Une personne à l'emploi d'une société minière dispose en effet d'une position privilégiée afin de saboter volontairement les infrastructures essentielles à la cybersécurité de l'organisation ou pour compromettre l'intégrité, la confidentialité ou la disponibilité des données de l'entreprise. Dans un autre ordre d'idées, un acteur interne d'une entreprise du secteur minier peut, de manière involontaire, et notamment en raison d'un manque de formation, adopter un comportement numérique inadéquat ayant pour effet de diminuer le niveau de cyberprotection de son organisation ou de porter atteinte à la sécurité des données dont dispose celle-ci.

L'éventail des conséquences potentielles découlant d'une cyberattaque fructueuse

Les impacts négatifs pouvant découler d'une cyberattaque fructueuse sont multiples et d'un niveau de gravité variable. Le **tableau 2** synthétise les principales conséquences pouvant découler d'une cyberattaque ayant réussi à affecter les infrastructures opérationnelles d'un site minier. Les éléments qui sont énumérés au **tableau 2** ne constituent cependant pas une liste exhaustive de toutes les conséquences possibles.

Tableau 2 – Conséquences possibles d'une cyberattaque affectant les infrastructures opérationnelles d'une entreprise minière

Conséquences sur la santé, la sécurité, l'environnement et les communautés	Conséquences pouvant entraîner l'interruption des activités	Conséquences commerciales et réputationnelles
Blessures sérieuses et dommages corporels	Perturbation de la chaîne d'approvisionnement	Pénalités, amendes et divulgation de contrats
Feux, explosions et autres dangers	Dommages aux équipements critiques	Perte d'opportunités et de revenu
Perturbation des activités	Suspension de la licence d'opérer	Dégradation de l'image de marque et de la réputation

Source : Ernst & Young et associés (2018).

Comme il est possible de le constater, les conséquences d'une cyberattaque affectant les infrastructures opérationnelles d'une entreprise minière peuvent se révéler néfastes sur de nombreux plans. D'abord, une cyberattaque affectant les infrastructures opérationnelles d'un complexe minier peut dérégler le processus de contrôle et de surveillance à distance des équipements mobiles et fixes. Les équipements ainsi compromis sont alors susceptibles de devenir une source de danger pour la santé et la sécurité de la main-d'œuvre. La perturbation des équipements opérationnels peut également entraîner des feux, des explosions ou d'autres dangers qui sont susceptibles non seulement de compromettre la sécurité du personnel, mais également de faire peser un risque sur l'environnement. Ensuite, les cyberattaques affectant les infrastructures opérationnelles d'une mine peuvent avoir des conséquences sur la productivité. En effet, tant la chaîne d'approvisionnement que les équipements critiques d'une mine peuvent se retrouver paralysés à la suite d'une cyberattaque fructueuse. Dans un tel contexte, la production minérale peut se voir ralentie ou même complètement arrêtée pendant une période de temps variable. Finalement, des conséquences commerciales et réputationnelles sont également possibles. En effet, le fait qu'une entreprise ait fait l'objet d'une cyberattaque fructueuse peut dégrader significativement son image et sa réputation tant auprès du grand public, des autorités publiques que des investisseurs. Par conséquent, des opportunités d'affaires peuvent être perdues et des sources de revenus compromises.

De plus, il est important de garder à l'esprit que les conséquences potentielles présentées au **tableau 2** et aux paragraphes précédents représentent les impacts possibles des cyberattaques réussissant à affecter les infrastructures opérationnelles d'une organisation. Les cyberattaques qui affectent uniquement les infrastructures informatiques d'une entreprise continuent de représenter une grande menace pour les organisations de l'ensemble des secteurs, dont le secteur minier. Les cyberattaques affectant uniquement les infrastructures informatiques se caractérisent généralement, lorsqu'elles sont fructueuses, par le vol, la destruction ou la compromission de l'intégrité des données, les tentatives d'extorsion d'argent et la perturbation des activités normales des organisations (CISCO, 2020).

La cybersécurité : une responsabilité collective

La cybersécurité représente donc l'un des enjeux majeurs que devra relever le secteur minier à l'ère de la quatrième révolution industrielle. Mais comment l'industrie minière peut-elle agir concrètement pour mettre en place des mesures efficaces en matière de cybersécurité? Selon un rapport de la firme de conseil Willis Towers Watson, au moins les deux tiers des cyberattaques fructueuses affectant les entreprises du secteur minier résultent d'un comportement inadéquat de la part du personnel (Austmine, 2018). Cette information est capitale, car elle signifie que malgré les infrastructures technologiques de cyberprotection mises en place par les équipes dédiées à la gestion des technologies de l'information, les entreprises du secteur minier demeurent vulnérables au cyberrisque en raison de la cyberhygiène parfois déficiente de leur personnel. Le professeur Foutse Khomh du département de génie informatique et génie logiciel à Polytechnique Montréal corrobore le fait que les infrastructures technologiques ne peuvent assurer à elles seules une cybersécurité optimale aux organisations. En effet, il soutient que « les entreprises pensent à tort être bien préparées pour faire face aux enjeux de sécurité. Elles semblent cantonner les problèmes de sécurité à une question d'infrastructures. Une approche holistique serait clairement plus efficace. Les enjeux de sécurité doivent être pris en compte tout au long du cycle de développement, de la mise en production jusqu'à l'utilisation des systèmes informatiques » (NOVIPRO & Léger, 2020, p. 10).

L’accroissement de la cyberhygiène observée par le personnel du secteur minier et l’amélioration des compétences en cybersécurité de ce dernier représentent donc un impératif pour rehausser la cybersécurité du secteur minier, et ce, d’autant plus que l’accélération du tournant de l’industrie des mines vers la quatrième révolution industrielle et la transformation numérique qui l’accompagne fait en sorte qu’une proportion croissante de la main-d’œuvre du secteur utilise des appareils et des outils technologiques connectés dans le cadre de son travail. Les outils tels que les appareils informatiques connectés, les équipements personnels connectés, les applications sont en effet d’ores et déjà largement utilisés dans le secteur minier, et tout indique que le recours à ceux-ci continuera à connaître une croissance au cours des années à venir (Forum économique mondial, 2017). Cette omniprésence des appareils connectés, tant dans le monde du travail que dans la sphère privée, fait en sorte que Sécurité publique Canada considère actuellement que « la cybersécurité était autrefois la chasse gardée d'experts techniques, mais [qu’]aujourd'hui, dans notre univers numérique, nous avons tous un rôle à jouer pour protéger notre cybersécurité individuelle et collective » (Sécurité publique Canada, 2018, p. 9).

La cybersécurité : Un concept à définir

Le domaine de la cybersécurité étant un secteur d’activités ainsi qu’un champ d’études relativement récents, la conceptualisation même de ce que constitue la cybersécurité reste encore l’objet de débats. D’ailleurs, plusieurs auteurs dénotent l’absence d'une définition uniformément acceptée à l’échelle internationale (Baylon, 2014; Schatz et al., 2017). Dans sa *Politique gouvernementale de cybersécurité*, le Secrétariat du Conseil du Trésor du Québec mentionne que la cybersécurité correspond à la « capacité, pour un système en réseau, de se protéger et de résister à des événements issus du cyberespace et susceptibles de porter atteinte à la confidentialité, à l’intégrité et à la disponibilité de l’information qu’il contient » (Secrétariat du Conseil du trésor, 2020, p. 2).

De son côté, Sécurité publique Canada postule au sein de sa *Stratégie nationale de cybersécurité* que « la cybersécurité est définie comme la protection de l'information

numérique et de l'infrastructure sur laquelle elle repose » (Sécurité publique Canada, 2018, p. 9).

Les professeurs Schatz, Bashroush et Wall de l'Université de Londres-Est ont, quant à eux, cherché à établir la définition la plus représentative possible de ce que constitue la cybersécurité, et ce, en mobilisant des techniques d'analyse lexicales et sémantiques (Schatz et al., 2017). Leur analyse, qui repose sur 28 définitions de la cybersécurité émanant de sources gouvernementales et académiques provenant d'une grande variété de pays, a permis l'élaboration d'une définition combinant les composantes centrales des définitions recensées. La définition qu'ils proposent est la suivante :

> « L'approche et les actions associées aux processus de gestion des risques de sécurité suivis par les organisations et les États pour protéger la confidentialité, l'intégrité et la disponibilité des données et des actifs utilisés dans le cyberespace. Le concept comprend les lignes directrices, les politiques […], les technologies, les outils et les formations utilisés pour fournir la meilleure protection à l'état du cyberenvironnement et à ses utilisateurs »[4] (Schatz et al., 2017).

La définition que Schatz, Bashroush et Wall mettent de l'avant présente une vision holistique de ce que constitue la cybersécurité, c'est celle-ci qui sera retenue pour orienter les analyses dans le présent rapport. Il apparaît donc qu'en matière de formation minière, le concept de « cybersécurité » doit être interprété au sens large et comme intégrant l'ensemble des approches et des actions visant le développement des compétences utiles à la protection de la confidentialité, de l'intégrité et de la disponibilité des données et des actifs utilisés dans le cyberespace.

Les compétences en cybersécurité dans le secteur minier du 21e siècle

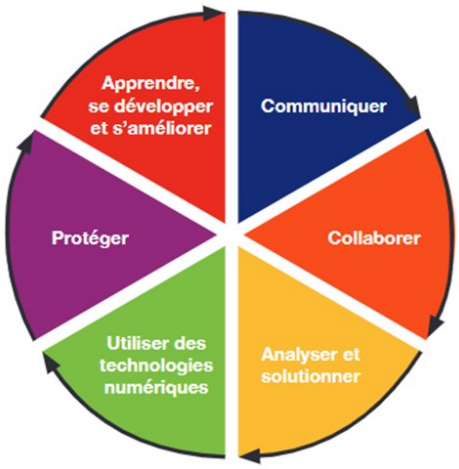
Pour les organisations, l'augmentation du niveau de cyberhygiène par l'entremise de l'amélioration des compétences en cybersécurité de la main-d'œuvre constitue une manière privilégiée d'accroître la cybersécurité, considérant le fait que « les brèches surviennent souvent de manière non intentionnelle, puisque trop d'employés manquent de formation pour détecter les pièges » (NOVIPRO & Léger, 2020, p. 16). Ce constat est d'autant plus vrai dans

[4] Traduction libre.

les secteurs d'activité, tel le secteur minier, où les technologies de pointe et connectées sont mobilisées de manière croissante. D'ailleurs, la firme de télécommunication Inmarsat mentionne, en se basant sur des entrevues réalisées auprès de 200 compagnies minières œuvrant partout à travers la planète, que les compétences en sécurité des données sont celles qui sont les plus recherchées par les entreprises du secteur minier pour permettre à la main-d'œuvre d'être apte à prendre le tournant de l'Internet des objets (Inmarsat, 2020). De plus, lorsque les mêmes entreprises se prononcent à propos de ce qu'elles conçoivent comme constituant leurs risques les plus importants en matière de cybersécurité, la crainte d'une mauvaise manipulation des données par des membres de leur personnel est citée par 54 % des répondantes (Inmarsat, 2020).

En 2020, la publication du *Cadre de référence des compétences à l'ère du numérique dans le secteur minier* a permis d'identifier vingt-trois actions-clés numériques nécessaires à maîtriser dans les mines à l'ère numérique afin d'être « numériquement compétent » (Institut national des mines et al., 2020). Ces vingt-trois actions-clés ont été regroupées en six familles de compétences. Comme il est possible de le constater à la **figure 1**, l'une des six familles s'intitule « Protéger » et correspond aux actions-clés associées à la protection face aux cyberattaques et à la prévention des cyberrisques.

Figure 1 – Les six familles de compétences numériques du « Cadre de référence des compétences à l'ère du numérique dans le secteur minier »



Source : Institut national des mines, Comité sectoriel de main-d'œuvre de l'industrie des mines et Association minière du Québec. (2020).

La famille de compétences qui s'intitule « Protéger » s'articule en quatre actions-clés distinctes. Ces quatre actions-clés peuvent être consultées au **tableau 3**. Dans le cadre de ce rapport, trois des quatre actions-clés constitutives de cette famille de compétences seront considérées comme faisant partie intégrante des compétences en cybersécurité devant être possédées par le personnel du secteur minier. Ces trois actions-clés sont :

1. Utiliser adéquatement et en toute sécurité les équipements numériques;

2. Protéger les données personnelles et corporatives;

3. Gérer les risques.

Bien que l'action-clé « Adopter des comportements virtuels appropriés » occupe également une place importante dans la protection numérique du secteur minier, celle-ci ne joue pas directement un rôle dans la prévention des cyberrisques auxquels fait face l'industrie minière. Cette action-clé n'est donc pas considérée dans le cadre de ce rapport.

Tableau 3 – La famille de compétences numériques « Protéger » selon « Le cadre de référence des compétences à l'ère du numérique dans le secteur minier »

PROTÉGER	Connaître les mesures de sécurité dans un environnement numérique, prendre en compte la fiabilité et la protection des données et protéger les appareils et le contenu numérique des véhicules autonomes.	**Utiliser adéquatement et en toute sécurité les équipements numériques** Utiliser de façon sécuritaire et préventive des équipements dans un environnement numérique.
		Protéger les données personnelles et corporatives (cybersécurité) Appliquer des lois et des politiques relatives à la protection des informations nominatives ou de l'entreprise.
		Adopter des comportements virtuels appropriés (cyber comportements) Se comporter avec éthique et dignité sur les réseaux sociaux ou dans ses échanges numériques.
		Gérer les risques Identifier les événements dont la concrétisation aurait un impact positif ou négatif sur le travail.

Source : Institut national des mines, Comité sectoriel de main-d'œuvre de l'industrie des mines et Association minière du Québec. (2020).

Méthodologie de recherche

La méthodologie utilisée afin de réaliser ce projet de stage s'appuie sur une approche quantitative. Dans un premier temps, une approche basée sur la revue de littérature a été mobilisée pour documenter l'importance de la cybersécurité dans le secteur minier à l'ère de la quatrième révolution industrielle et de la mine intelligente. Dans un second temps, une collecte de données quantitative a été menée. Celle-ci a été effectuée à l'aide d'un questionnaire abordant deux grandes questions : d'abord, les personnes apprenantes sont-elles sensibilisées aux actions-clés relatives à la cybersécurité dans les programmes de formation minière au Québec. Ensuite, quelle est la perception des établissements d'enseignement à l'égard de la cybersécurité.

Méthodologie de la collecte de données

Le questionnaire[5] a été élaboré au printemps 2020 par nous-même. La plateforme sur laquelle le questionnaire a été développé est la plateforme de sondage en ligne *Survey Monkey*. Le questionnaire comptait vingt et une questions et le temps moyen de remplissage de la part des personnes répondantes était d'environ dix minutes. Les établissements d'enseignement sélectionnés pour participer à la collecte de données ont été contactés afin qu'un membre de leur personnel possédant une expertise dans le programme de formation professionnelle ou le programme d'études collégiales ciblé soit désigné pour répondre au questionnaire. Les personnes répondantes ainsi désignées dans chaque organisation ont ensuite été jointes par courriel par nous-même afin de recevoir des explications quant à la nature de la collecte de données et se sont vu transmettre le questionnaire. La collecte de données s'est échelonnée sur une période de plus de quatre mois s'étendant du 14 mai 2020 au 24 septembre 2020.

Échantillonnage

Pour délimiter l'étendue de la recherche, il a été décidé que les trois programmes de formation professionnelle et les trois programmes d'études collégiales menant à l'exercice des métiers et professions qui sont les plus en demande dans le secteur minier du Québec

[5] Le questionnaire est disponible en **Annexe I**.

seraient analysés dans le cadre de cette collecte de données. La décision de privilégier l'étude des programmes de formation professionnelle et des programmes d'études collégiales qui sont les plus en demande dans le secteur minier du Québec repose sur le fait que 78 % des postes à pourvoir dans le secteur minier québécois à l'horizon de 2023 nécessiteront soit la possession d'un diplôme d'études professionnelles (DEP), soit celle d'un diplôme d'études collégiales (DEC) (Comité sectoriel de main-d'oeuvre de l'industrie des mines, 2020, p. 17).

Pour cibler les programmes de formation et les programmes d'études devant être analysés dans le cadre de cette collecte de données, l'étude *Estimation des besoins de main-d'œuvre du secteur minier au Québec 2019-2023 avec tendances 2028* a été utilisée (CSMO Mines, 2020). L'ensemble des établissements d'enseignement situés dans les trois principales régions minières du Québec (l'Abitibi-Témiscamingue, la Côte-Nord et le Nord-du-Québec) offrant l'un ou plusieurs des programmes de formation et d'études identifiés dans le rapport du comité sectoriel de la main-d'œuvre de l'industrie des mines ont été inclus dans la collecte de données[6].

De plus, puisque le DEC en technologie minérale n'est offert que dans un seul établissement d'enseignement (c'est-à-dire le Cégep de Thetford) en dehors des trois régions précédemment citées, la formation technique offerte par ce Cégep situé dans la région administrative de Chaudière-Appalaches a également été prise en considération dans la collecte de données. Une autre orientation méthodologique prise dans le cadre de cette collecte de données a consisté à ne pas prendre en considération les emplois de nature administrative afin de centrer ce rapport sur les formations menant à l'exercice d'un métier ou d'une profession directement liée à l'exploration minière, à l'extraction du minerai ou au traitement de celui-ci. En ce qui concerne les métiers exigeant un diplôme d'études professionnelles, un ajustement a été réalisé pour le métier d'opératrices et d'opérateurs de machinerie lourde spécialisée puisque la formation la plus demandée pour occuper ce poste, qui est le DEP en conduite d'engins de chantier, n'est pas offerte de manière récurrente par

[6] Selon l'Institut de la statistique du Québec, les trois principales régions minières du Québec sont le Nord-du-Québec, l'Abitibi-Témiscamingue et la Côte-Nord. En effet, ces trois régions « fournissent la majorité des emplois dans le secteur minier, soit 63,8 % des emplois pour l'ensemble du Québec » et « se partagent 95,2 % des investissements [miniers] totaux au Québec en 2018 » (Institut de la statistique du Québec, 2019, 2020).

les centres de formation professionnelle présents sur les territoires de l'Abitibi-Témiscamingue, de la Côte-Nord et du Nord-du-Québec. Le DEP de conduite de machinerie lourde en voirie forestière, qui est quant à lui dispensé dans ces trois régions, a donc remplacé le DEP en conduite d'engins de chantier dans l'échantillon. Le **Tableau 4** présente les établissements d'enseignement offrant les programmes de formation et les programmes d'études participant à cette collecte de données.

Tableau 4 – Établissements d'enseignement interrogés

Formation collégiale	
Programmes d'études	**Établissements d'enseignement**
1. DEC – Technologie minérale – Spécialisation en géologie	• Cégep de l'Abitibi-Témiscamingue • Cégep de Sept-Îles • Cégep de Thetford
2. DEC – Technologie de l'électronique industrielle	• Cégep de l'Abitibi-Témiscamingue • Cégep de Baie-Comeau • Cégep de Sept-Îles
3. DEC – Technologie minérale – Spécialisation en exploitation	• Cégep de l'Abitibi-Témiscamingue • Cégep de Sept-Îles • Cégep de Thetford
Formation professionnelle	
Programmes de formation	**Établissements d'enseignement**
1. DEP – Conduite de machinerie lourde en voirie forestière	• Centre de formation professionnelle de la Baie-James • Centre de formation professionnelle de l'Estuaire • Centre de formation professionnelle Harricana
2. DEP – Extraction de minerai	• Centre de formation professionnelle de la Baie-James • Centre de formation professionnelle Val-d'Or
3. DEP – Mécanique d'engins de chantier	• Centre de formation professionnelle de la Baie-James • Centre de formation professionnelle Lac-Abitibi • Centre de formation professionnelle de Sept-Îles

Le **tableau 5** permet de constater que les personnes répondantes désignées par les établissements d'enseignement pour répondre au questionnaire sont majoritairement des

enseignantes et des enseignants, mais que du personnel professionnel a également été mandaté pour ce faire.

Tableau 5 – Fonction occupée par les personnes répondantes dans les établissements d'enseignement

CHOIX DE RÉPONSES	RÉPONSES	
Enseignante ou enseignant	70.59%	12
Professionnelle ou professionnel	29.41%	5
Personnel de soutien	0.00%	0
Personnel d'encadrement	0.00%	0
Autre (veuillez préciser)	0.00%	0
TOTAL		17

Question : « Quelle est votre fonction? »

L'ensemble des dix établissements d'enseignement sollicités pour remplir le questionnaire ont répondu favorablement à notre demande de participation, ce qui signifie que les six programmes analysés dans le cadre de ce rapport ont obtenu les réponses de trois établissements d'enseignement différents, exception faite du programme d'*Extraction de minerai* qui n'est offert que par deux établissements scolaires au Québec. Au total, dix-sept personnes répondantes ont donc rempli le questionnaire, c'est-à-dire une personne répondante par programme et par établissement. Ces chiffres correspondent à un taux de réponse de 100 % de la part des établissements d'enseignement contactés.

Résultats

Rappelons que l'objectif de ce rapport de stage est de répondre à deux grandes questions liées à la formation minière offerte dans les centres de formation professionnelle et les cégeps du Québec. D'abord, quelle est la place de la cybersécurité dans la formation minière québécoise. En d'autres mots, est-ce que les personnes apprenantes se destinant à travailler dans le secteur minier sont sensibilisées à la cybersécurité? Ensuite, quelle perception les établissements d'enseignement du Québec offrant de la formation minière ont-ils de la cybersécurité?

La sensibilisation aux actions-clés relatives à la cybersécurité dans la formation minière au Québec

Dans l'optique d'évaluer à quel point l'enseignement offert dans ces programmes de formation sensibilise les personnes apprenantes à la cybersécurité, la place occupée par les trois actions-clés considérées comme jouant un rôle direct dans la prévention des cyberrisques a été évaluée.

Tout d'abord, l'enquête permet de déterminer dans quelle mesure les personnes apprenantes sont sensibilisées à l'action-clé « Utiliser adéquatement et en toute sécurité les équipements numériques ». Le **tableau 6** permet de constater que la majorité des personnes répondantes, soit 58,82 % d'entre elles, soulignent être « Peu » ou « Pas du tout » en accord avec l'assertion selon laquelle « les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques » au cours de leur parcours en formation minière. De plus, 41,18 % des personnes répondantes affirment être « Assez en accord » avec cette dernière assertion.

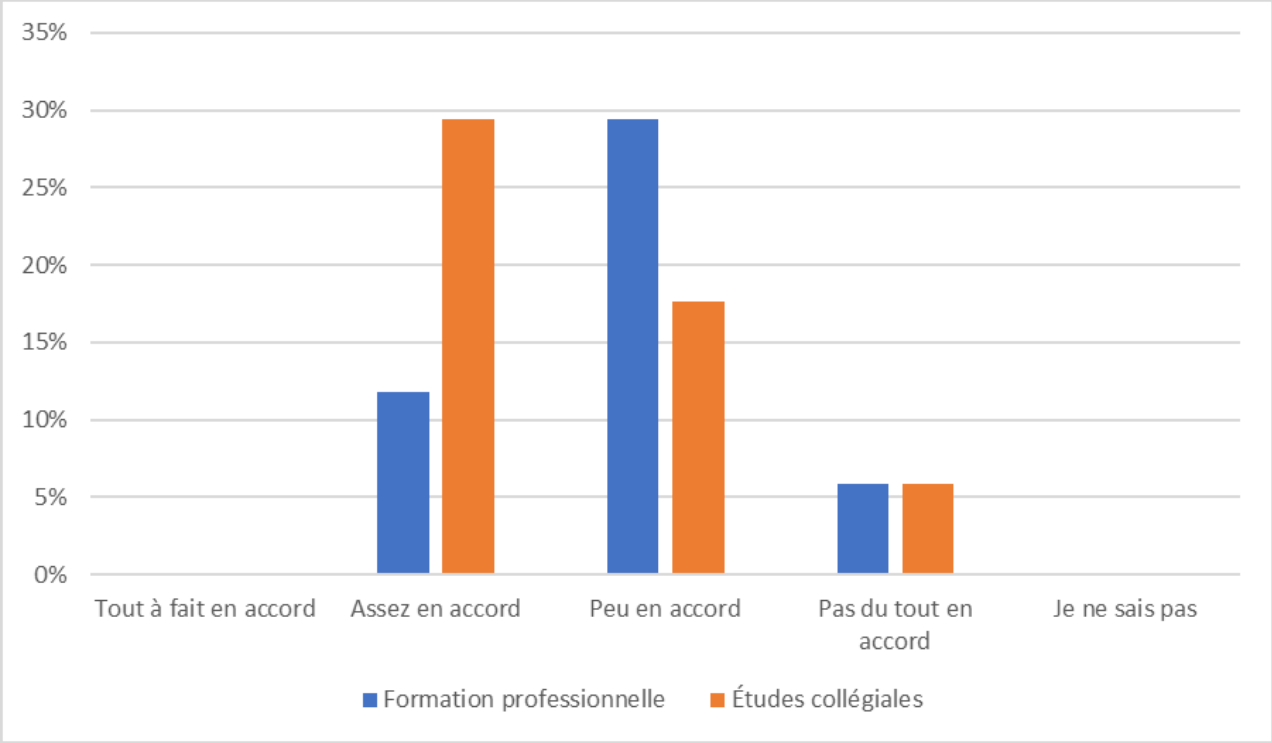
Tableau 6 – Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques

CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait en accord	0.00%	0
Assez en accord	41.18%	7
Peu en accord	47.06%	8
Pas du tout en accord	11.76%	2
Je ne sais pas	0.00%	0
TOTAL		17

Question : « Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : dans le cadre du programme d'études actuellement en vigueur, les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques (exemple : gestion des mots de passe). »

Une analyse plus en profondeur des résultats permet de discerner des variations entre la sensibilisation à l'utilisation sécuritaire et préventive des équipements numériques réalisée en formation professionnelle et celle menée au sein de la formation collégiale. En effet, comme l'illustre la **figure 2**, les personnes répondantes émanant des programmes d'études collégiales sont prédominantes parmi les répondantes et les répondants considérant être « Assez en accord » avec l'énoncé selon lequel les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques, tandis que les personnes répondantes qui affirment être « Peu en accord» ou « Pas du tout en accord » avec cette assertion proviennent surtout de la formation professionnelle. Les données collectées indiquent donc que la sensibilisation des personnes apprenantes à l'action-clé « Utiliser adéquatement et en toute sécurité les équipements numériques » est effectuée dans la majorité de la formation minière collégiale analysée dans le cadre de ce rapport (55,6 % des personnes répondantes de cet ordre d'enseignement mentionnent être « Assez en accord »), mais que la situation est différente dans la formation professionnelle où seulement une faible proportion des personnes répondantes indiquent que leurs élèves sont sensibilisés à cette action-clé (25 % des personnes répondantes de cet ordre d'enseignement signalent être « Assez en accord »).

Figure 2 – Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques



Question : *« Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : dans le cadre du programme d'études actuellement en vigueur, les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques (exemple : gestion des mots de passe). »*

Ensuite, l'enquête permet de constater dans quelle mesure la sensibilisation à l'action-clé « Protéger les données personnelles et corporatives » est présente dans les six programmes de formation et d'études analysés dans ce rapport. Le **tableau 7** montre que 52,94 % des personnes répondantes soutiennent être « Peu » ou « Pas du tout » en accord avec l'affirmation selon laquelle « les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations personnelles ou de l'entreprise » durant leur formation. Il y a toutefois 47,06 % des personnes répondantes qui se déclarent « Assez en accord » avec cette assertion.

Tableau 7 – Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations

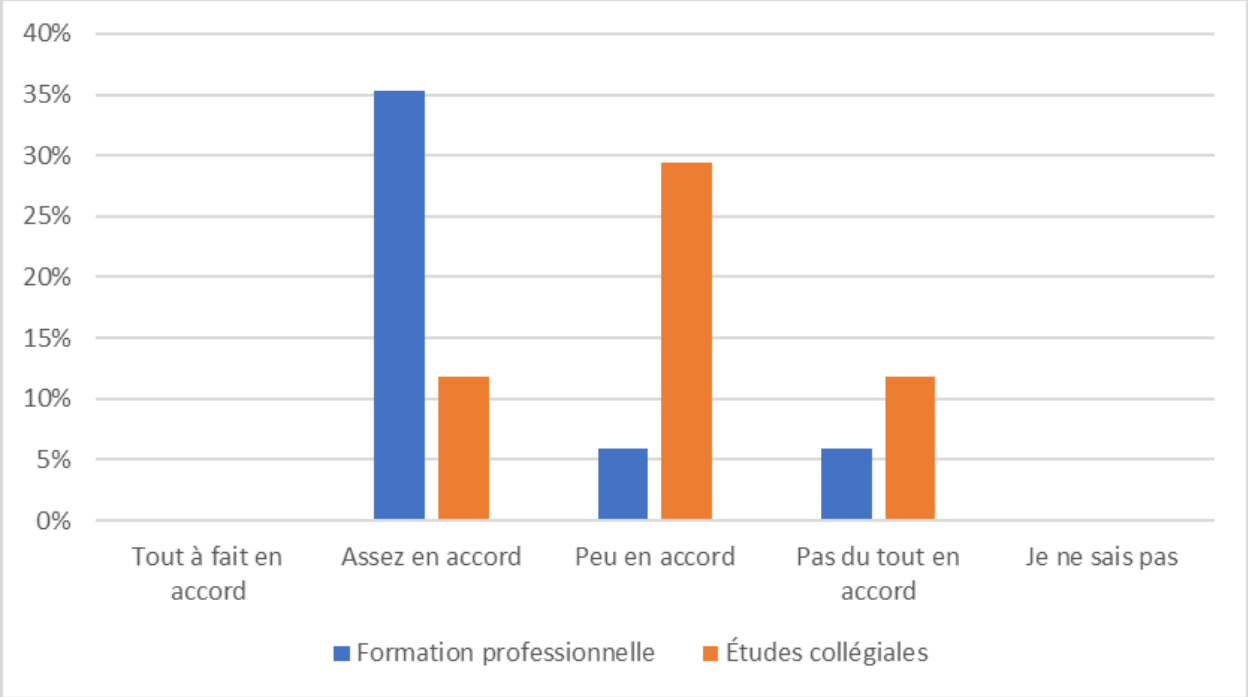
CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait en accord	0.00%	0
Assez en accord	47.06%	8
Peu en accord	35.29%	6
Pas du tout en accord	17.65%	3
Je ne sais pas	0.00%	0
TOTAL		17

Question : *« Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : dans le cadre du programme d'études actuellement en vigueur, les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations personnelles ou de l'entreprise. »*

Tout comme lors de l'examen de l'action-clé précédente, les résultats de l'enquête révèlent des disparités entre la sensibilisation à l'importance d'appliquer les lois et les politiques relatives à la protection des informations accomplie en formation professionnelle et celle réalisée dans la formation collégiale. Comme l'indique la **figure 3**, les personnes répondantes provenant des centres de formation professionnelle sont majoritaires parmi les répondantes et les répondants considérant être « Assez en accord » avec l'énoncée selon laquelle les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations alors que les personnes répondantes qui affirment être « Peu en accord» ou « Pas du tout en accord » sont surtout issues de la formation collégiale. La **figure 3** permet de constater que la sensibilisation des personnes apprenantes à l'action-clé « Protéger les données personnelles et corporatives » est effectuée dans la majorité de la formation minière de niveau professionnel analysé dans le cadre de ce rapport (75 % des personnes répondantes de cet ordre d'enseignement indiquent être « Assez en accord »). La réalité est toute autre dans la formation collégiale où seulement une faible proportion des personnes répondantes indiquent que leurs personnes apprenantes sont

sensibilisés aux notions reliées à cette action-clé (25 % des personnes répondantes de cet ordre d'enseignement spécifient être « Assez en accord »).

Figure 3 – Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations



Question : *« Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : dans le cadre du programme d'études actuellement en vigueur, les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations personnelles ou de l'entreprise. »*

Par la suite, l'enquête établit dans quelle mesure la sensibilisation à l'action-clé « Gérer les risques » se retrouve dans les programmes de formation analysés. Le **tableau 8** expose que 76,47 % des personnes répondantes mentionnent être « Peu » ou « Pas du tout » en accord avec l'affirmation selon laquelle « les personnes apprenantes sont sensibilisées à la gestion des risques numériques notamment par l'identification des événements pouvant avoir un impact sur le travail » au cours de leur cheminement. En ce qui concerne les personnes répondantes qui sont « Assez en accord » avec cette assertion, il est possible de constater que celles-ci ne représentent que 17,65 %.

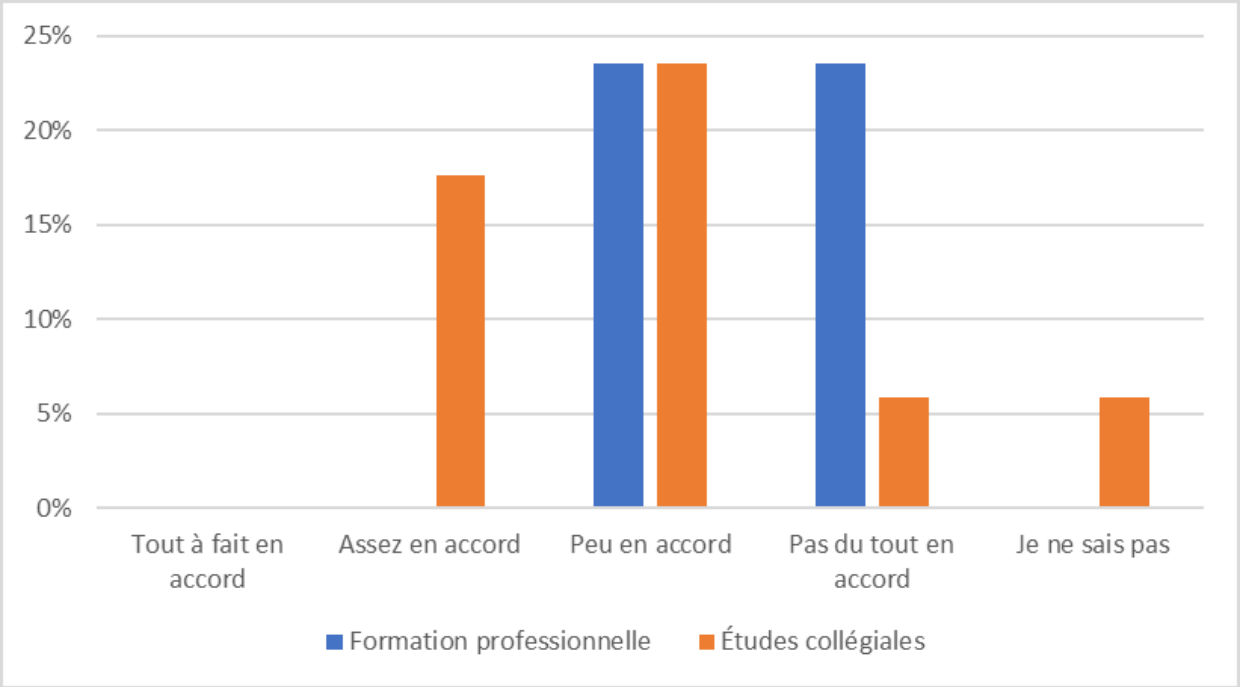
Tableau 8 – Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à la gestion des risques numériques

CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait en accord	0.00%	0
Assez en accord	17.65%	3
Peu en accord	47.06%	8
Pas du tout en accord	29.41%	5
Je ne sais pas	5.88%	1
TOTAL		17

Question : *« Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : dans le cadre du programme d'études actuellement en vigueur, les personnes apprenantes sont sensibilisées à la gestion des risques numériques notamment par l'identification des événements pouvant avoir un impact sur le travail (exemple : identifier et rapporter les incidents de cybersécurité, reconnaître un courriel d'hameçonnage, etc.). »*

Encore une fois, les données recueillies offrent la possibilité d'analyser la sensibilisation à la gestion des risques numériques qui est réalisée par chacun des ordres d'enseignement. La **figure 4** expose à cet effet que les seules personnes répondantes qui mentionnent être « Assez en accord » avec l'assertion selon laquelle les personnes apprenantes sont sensibilisées à la gestion des risques numériques proviennent des cégeps. En effet, l'ensemble des personnes répondantes de la formation professionnelle signalent être « Peu en accord » ou encore « Pas du tout en accord » avec cet énoncé. La sensibilisation des personnes apprenantes à l'action-clé « Gérer les risques » apparaît donc comme très peu présente dans les programmes de formation professionnelle analysés, car aucune des personnes répondantes de cet ordre d'enseignement n'a indiqué être « Assez en accord ». En ce qui a trait à la sensibilisation à l'action-clé « Gérer les risques » en formation collégiale, un total de 33,33 % des personnes répondantes de cet ordre d'enseignement ont souligné être « Assez en accord ».

Figure 4 – Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à la gestion des risques numériques



Question : *« Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : dans le cadre du programme d'études actuellement en vigueur, les personnes apprenantes sont sensibilisées à la gestion des risques numériques notamment par l'identification des événements pouvant avoir un impact sur le travail (exemple : identifier et rapporter les incidents de cybersécurité, reconnaître un courriel d'hameçonnage, etc.). »*

Finalement, l'enquête évalue si, au-delà de la sensibilisation aux trois actions-clés numériques retenues, d'autres notions relatives à la cybersécurité sont mises de l'avant dans les six programmes de formation et d'études analysés. Le **tableau 9** permet de constater que seulement une personne répondante a mentionné que de telles notions sont présentes dans le cadre du programme d'études actuellement en vigueur. Ainsi, un seul programme, offert dans un seul établissement, inclut l'apprentissage de notions de cybersécurité supplémentaires par rapport à celles contenues dans la famille de compétences « Protéger ». La seule réponse affirmative au **tableau 9** provient de l'ordre d'enseignement collégial.

Tableau 9 – Instauration d'autres activités ayant pour but la sensibilisation à toute notion relative à la cybersécurité

CHOIX DE RÉPONSES	RÉPONSES	
oui	5.88%	1
non	94.12%	16
TOTAL		17

Question : « *Avez-vous, dans le cadre du programme d'études actuellement en vigueur, instauré toute autre activité ayant pour but la sensibilisation à toute notion relative à la cybersécurité? »*

L'examen des résultats précédents permet de dégager une vision globale de la sensibilisation aux actions-clés en cybersécurité des personnes apprenantes inscrites dans les six programmes de formation et d'études analysés dans le cadre de ce présent rapport. Il apparaît que l'action-clé « Protéger les données personnelles et corporatives » est celle à laquelle les personnes apprenantes sont la plus sensibilisée, suivi de l'action-clé « Utiliser adéquatement et en toute sécurité les équipements numériques » et enfin de l'action-clé « Gérer les risques ». Il est également intéressant de noter qu'en ce qui concerne chacune de ces actions-clés, la majorité des personnes répondantes jugent que les personnes apprenantes y sont « Peu » ou « Pas du tout » sensibilisées. Finalement, il est aussi possible de poser le constat que la mention « Tout à fait d'accord » n'apparaît pas aux **tableaux 6**, **7** et **8**. Cela semble signifier qu'aucune personne répondante ne considère que la sensibilisation à l'égard des trois actions-clés fondamentales en cybersécurité dans le secteur minier n'est réalisée de manière optimale dans le cadre du programme de formation ou d'études actuellement en vigueur.

L'examen des résultats de l'enquête offre également l'opportunité de faire une analyse par ordre d'enseignement des données collectées. L'étude des **figures 2**, **3** et **4** révèle que la sensibilisation à la cybersécurité pour deux des trois actions-clés en cybersécurité analysées dans le cadre de ce rapport est prédominante dans les programmes d'études collégiales. De plus, le **tableau 9** permet de constater que le seul programme mettant de l'avant l'apprentissage de notions de cybersécurité complémentaires aux trois actions-clés de base

est un programme d'études collégiales. L'analyse des éléments précédents semblent donc indiquer que les trois programmes de formation collégiale analysés sensibilisent davantage leurs étudiantes et leurs étudiants aux actions-clés en cybersécurité de la famille de compétences « Protéger » du *Cadre de référence des compétences à l'ère du numérique dans le secteur minier* comparativement aux trois programmes de formation professionnelle étudiés. Il faut toutefois souligner que ce constat ne signifie pas que la sensibilisation aux notions de cybersécurité est absente des programmes de formation professionnelle examinés. En effet, les données collectées indiquent que les programmes de formation professionnelle sensibilisent davantage aux notions reliées à l'action-clé « Protéger les données personnelles et corporatives » que les programmes d'études collégiales.

La perception des établissements d'enseignement quant à l'importance de la cybersécurité en formation minière

Dans le cadre de ce rapport, nous avons également cherché à déterminer la perception des établissements d'enseignement sondés à l'importance accordée à la cybersécurité et à l'apprentissage des compétences reliées à celle-ci. Pour ce faire, les questions 13 à 17 du questionnaire ont été analysées.

Tout d'abord, le questionnaire a permis d'évaluer dans quelle mesure les personnes répondantes estiment probable qu'au moins une activité pédagogique reliée à la cybersécurité soit instaurée dans leur programme de formation ou d'études au cours des deux prochaines années. Le **tableau 10** permet de constater que la majorité des personnes répondantes, c'est-à-dire 76,47 % d'entre elles, estiment qu'il est « Très probable » ou « Assez probable » qu'une activité pédagogique de ce type soit incluse dans la formation offerte aux personnes apprenantes inscrites à l'une des six formations analysées. Près d'une personne répondante sur quatre (23,53 %) juge quant à elle « Peu probable » que soient instaurées une ou plusieurs activités pédagogiques visant à sensibiliser les personnes apprenantes à la cybersécurité à l'horizon 2022.

Tableau 10 – Probabilité d'instauration d'activités pédagogiques sensibilisant à la cybersécurité au cours des deux prochaines années

CHOIX DE RÉPONSES	RÉPONSES	
Très probable	35.29%	6
Assez probable	41.18%	7
Peu probable	23.53%	4
Très peu probable	0.00%	0
Pas du tout probable	0.00%	0
TOTAL		17

Question : *« Au cours des deux prochaines années, est-il probable que soient instaurées une ou plusieurs activités pédagogiques visant à sensibiliser les personnes apprenantes à la cybersécurité dans le cadre du programme d'études actuellement en vigueur? »*

Par la suite, l'enquête a cherché à établir la perception à l'égard de l'importance de la cybersécurité dans le secteur minier. Les résultats présentés au **tableau 11** montrent une tendance claire puisque l'ensemble des répondantes et des répondants ont indiqué considérer comme « Très important » (64,71 %) ou « Assez important » (35,29 %) le niveau d'importance que le secteur minier devrait accorder à la cybersécurité dans ses activités.

Tableau 11 – Perception du niveau d'importance que le secteur minier doit accorder à la cybersécurité dans ses activités

CHOIX DE RÉPONSES	RÉPONSES	
Très important	64.71%	11
Assez important	35.29%	6
Peu important	0.00%	0
Très peu important	0.00%	0
Pas du tout important	0.00%	0
TOTAL		17

Question : *« Selon vous, quel niveau d'importance le secteur minier doit-il accorder à la cybersécurité dans ses activités? »*

Dans le cadre de la collecte de données réalisée, les personnes répondantes ont indiqué, par rapport au programme de formation ou d'études dans lequel elles sont des experts de contenu, dans quelle mesure elles jugent nécessaire pour les personnes apprenantes inscrites dans le programme de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier. Le **tableau 12** révèle que la majorité des personnes répondantes (64,71 %) perçoivent que cela est « Très nécessaire » ou « Assez nécessaire ». Il est toutefois intéressant de soulever le fait que la proportion de personnes répondantes qui voient le développement de ces compétences comme « Assez nécessaire » (47,06 %) est significativement plus élevée que celle qui estime que ce développement de compétences est « Très nécessaire » (17,65 %). De leur côté, les répondantes et les répondants qui trouvent « Peu nécessaire » le développement de compétences en cybersécurité par les personnes apprenantes pour occuper des postes dans le secteur minier représentent 35,29 % des personnes répondantes.

Tableau 12 – Perception de la nécessité de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier

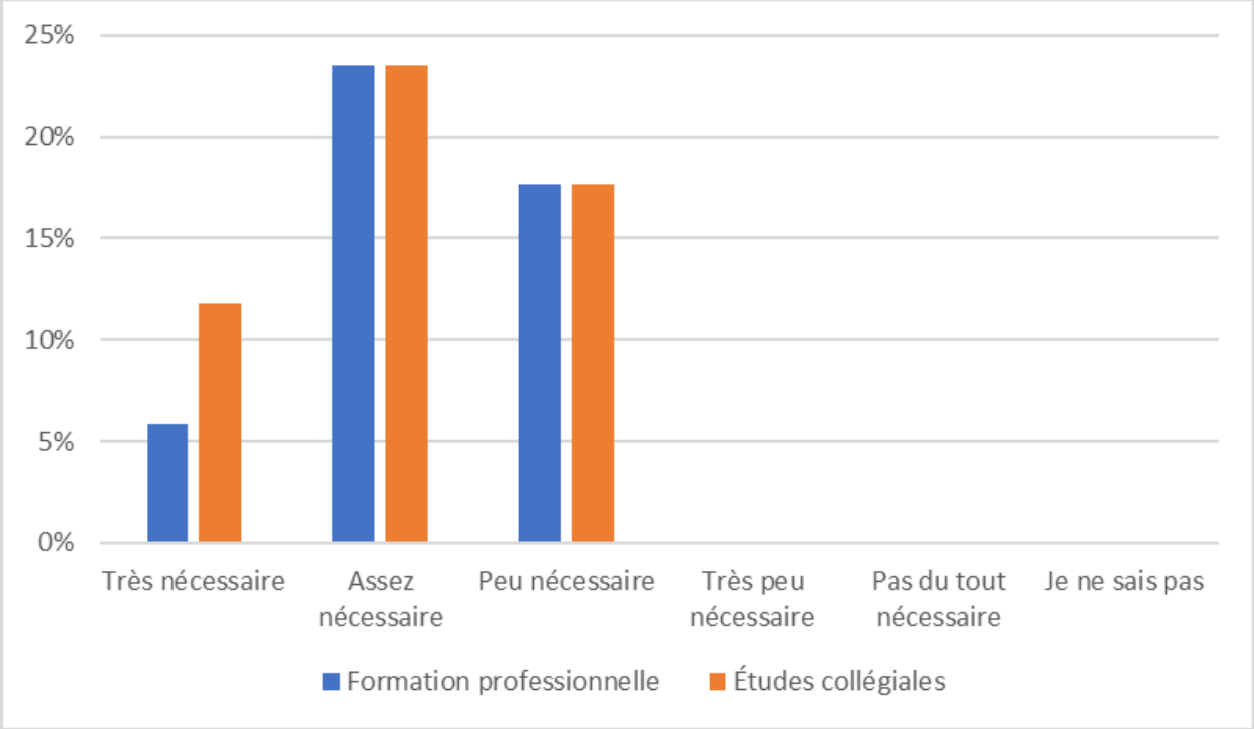
CHOIX DE RÉPONSES	RÉPONSES	
Très nécessaire	17.65%	3
Assez nécessaire	47.06%	8
Peu nécessaire	35.29%	6
Très peu nécessaire	0.00%	0
Pas du tout nécessaire	0.00%	0
Je ne sais pas	0.00%	0
TOTAL		17

Question : *« Selon vous, est-il nécessaire aux personnes apprenantes actuellement inscrites à ce programme de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier? »*

La **figure 5** permet de constater que l'opinion des personnes répondantes à l'égard de cette question ne diffère que très peu en fonction de l'ordre d'enseignement. En effet, la proportion de personnes répondantes des deux ordres d'enseignement indiquant qu'il est « Assez nécessaire » et « Peu nécessaire » pour les personnes apprenantes actuellement inscrites en

formation minière de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier est similaire. La proportion de personnes répondantes qui jugent qu'il est « Très nécessaire » de développer des compétences en cybersécurité est quant à elle légèrement plus élevée au collégial (22,2 %) qu'en formation professionnelle (12,5 %). Ces résultats illustrent le fait que les répondantes et les répondants de la formation professionnelle et de la formation collégiale ont une conception plutôt semblable de la nécessité de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier.

Figure 5 – Perception, par ordre d'enseignement, de la nécessité de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier



Question : *« Selon vous, est-il nécessaire aux personnes apprenantes actuellement inscrites à ce programme de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier? »*

L'enquête a aussi permis de mesurer la perception des personnes répondantes à l'égard du niveau de compétence en cybersécurité que devraient posséder les personnes apprenantes pour occuper des postes dans le secteur minier. Chacune des répondantes et chacun des répondants ont ainsi indiqué quel niveau de compétence en cybersécurité devrait détenir les personnes apprenantes inscrites au programme dans lequel il détient une expertise

pédagogique. Le **tableau 13** montre qu'aucune personne répondante n'estime que les personnes apprenantes en formation minière doivent posséder un « Niveau expert » ou « Aucun niveau » pour occuper des postes dans le secteur minier. Les réponses se situent en effet entre ces deux positions puisque 11,76 % des personnes répondantes indiquent qu'un « Niveau avancé » est nécessaire, contre 47,06 % qui préconisent un « Niveau intermédiaire » et 41,18 % qui évaluent qu'un « Niveau de base » est suffisant.

Tableau 13 – Perception du niveau de compétence en cybersécurité devant être possédée pour occuper des postes dans le secteur minier

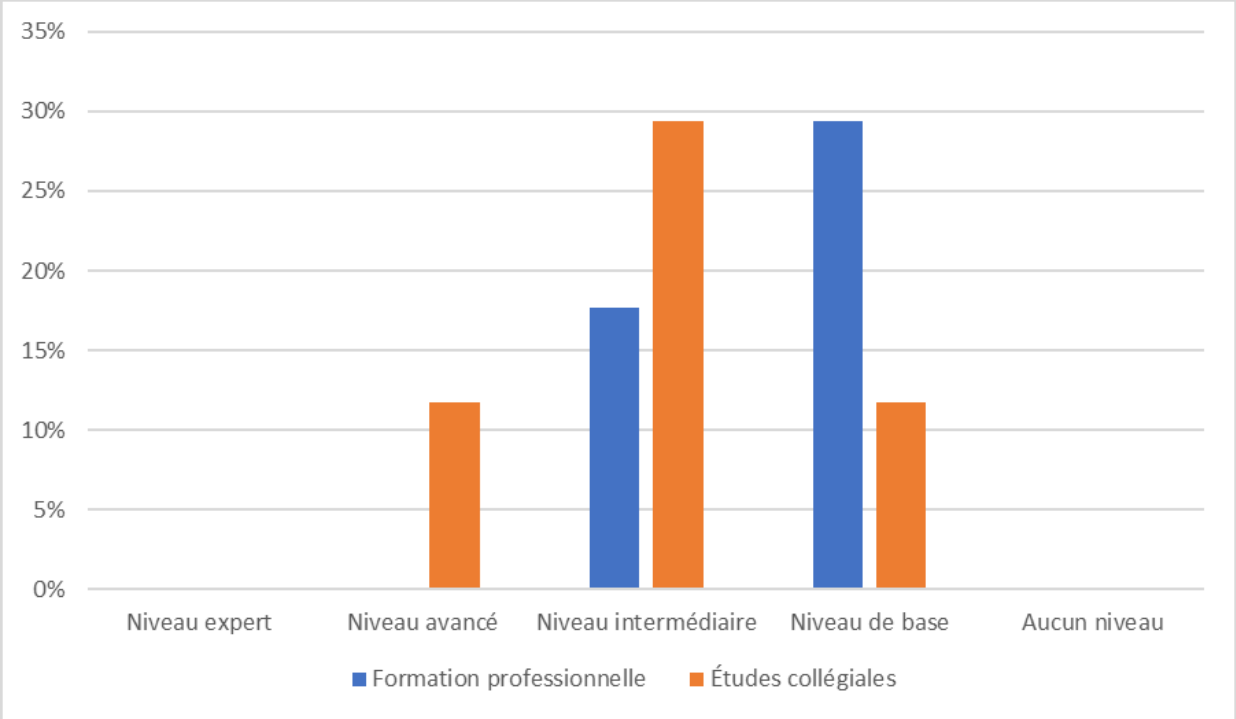
CHOIX DE RÉPONSES	RÉPONSES	
Niveau expert	0.00%	0
Niveau avancé	11.76%	2
Niveau intermédiaire	47.06%	8
Niveau de base	41.18%	7
Aucun niveau	0.00%	0
TOTAL		17

Question : *« Selon vous, quel niveau de compétence en cybersécurité devrait posséder les personnes apprenantes inscrites à ce programme pour occuper des postes dans le secteur minier? »*

Les données présentées au **tableau 13** peuvent également être analysées en fonction de l'ordre d'enseignement. Cette approche offre l'opportunité de mettre à jour les disparités entre les formations professionnelle et collégiale en ce qui a trait à la perception du niveau de compétence en cybersécurité devant être possédée par les personnes apprenantes pour occuper des postes dans le secteur minier. La **figure 6** expose que la majorité des personnes répondantes de la formation professionnelle évaluent que les élèves doivent posséder un « niveau de base » en cybersécurité tandis que la majorité des personnes répondantes de la formation collégiale estiment que les étudiantes et les étudiants doivent détenir un « niveau intermédiaire » en cybersécurité pour occuper des postes dans le domaine minier. Ces résultats mettent en lumière le fait que les expertes et les experts de contenu répondant pour la formation collégiale considèrent dans une proportion significativement plus importante

que leurs homologues de la formation professionnelle qu'un niveau « avancé » ou « intermédiaire » de compétence en cybersécurité est requis pour évoluer dans le secteur minier (cette proportion s'élève à 77,78 % au collégial et à 37,5 % en formation professionnelle). Cette réalité s'illustre également par le fait que seules des personnes répondantes du niveau collégial jugent qu'un « niveau avancé » de compétence en cybersécurité doit être possédé par les personnes apprenantes pour occuper des postes dans le domaine des mines.

Figure 6 – Perception, par ordre d'enseignement, du niveau de compétence en cybersécurité devant être possédé pour occuper des postes dans le secteur minier



Question : *« Selon vous, quel niveau de compétence en cybersécurité devrait posséder les personnes apprenantes inscrites à ce programme pour occuper des postes dans le secteur minier? »*

Finalement, la collecte de données a permis de recueillir l'opinion des personnes répondantes en ce qui concerne l'opportunité d'inclure l'acquisition d'une compétence reliée à la cybersécurité dans la prochaine mise à jour du devis ministériel du programme de formation ou d'études. Le **tableau 14** illustre que les personnes répondantes sont dans leur majorité plutôt en accord avec le principe d'inclure une telle compétence dans les devis ministériels

des programmes ciblés dans le cadre de ce rapport. En effet, 29,41 % d'entre elles soulignent être « Tout à fait en accord » avec cette idée et 47,06 % mentionnent être « Assez en accord ». À l'opposé, 11,76 % des répondantes et des répondants signalent être « Peu en accord » avec cette inclusion et 11,76 % sont même « Très peu en accord » avec cette perspective. Il est à noter qu'aucune personne répondante n'a indiqué être « Pas du tout en accord » avec l'idée.

Tableau 14 – Niveau d'accord avec l'idée d'inclure l'acquisition d'une compétence reliée à la cybersécurité dans le devis ministériel

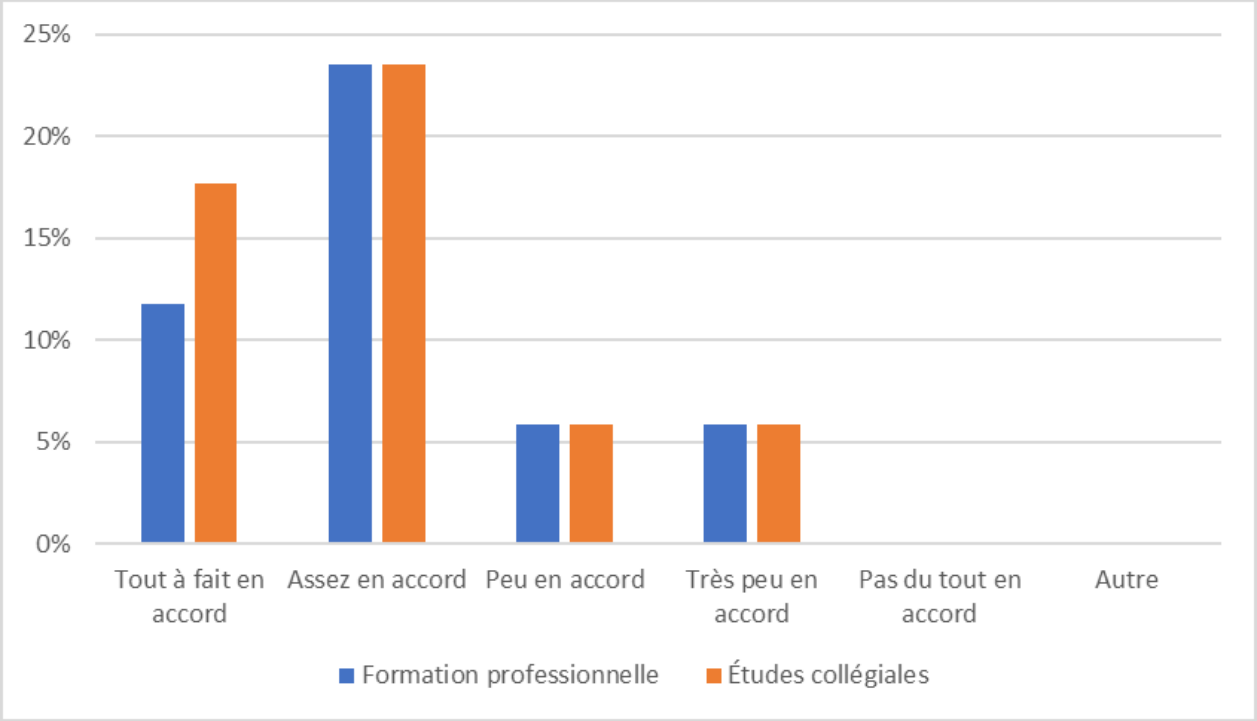
CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait en accord	29.41%	5
Assez en accord	47.06%	8
Peu en accord	11.76%	2
Très peu en accord	11.76%	2
Pas du tout en accord	0.00%	0
Autre (veuillez préciser)	0.00%	0
TOTAL		17

Question : *« Veuillez indiquer votre niveau d'accord avec l'énoncé suivant : la prochaine mise à jour de ce programme par le ministère de l'Éducation et de l'Enseignement supérieur devrait inclure l'acquisition d'une compétence reliée à la cybersécurité. »*

L'examen des données du **tableau 14** en fonction du programme de formation ou d'études au nom duquel les personnes répondantes ont complété l'enquête permet de déceler si des tendances sont observables entre les réponses émanant de la formation professionnelle et celles provenant de la formation collégiale. La **figure 7** montre qu'il existe peu de disparités entre les deux ordres d'enseignement concernant l'idée d'inclure l'acquisition d'une compétence reliée à la cybersécurité dans le devis ministériel des programmes de formation minière. En effet, 75 % des personnes répondantes de la formation professionnelle s'estiment « Tout à fait en accord » ou « Assez en accord » avec l'idée que l'acquisition d'une telle compétence soit ajoutée au devis ministériel tandis que cette proportion s'élève à 77,78 % au

niveau de la formation collégiale. Ces résultats illustrent le fait que bien que les deux ordres d'enseignement n'aient pas nécessairement la même perception du niveau de compétence en cybersécurité devant posséder les personnes apprenantes se destinant à occuper un emploi dans le secteur minier, ils considèrent tout de même dans une proportion semblable qu'une compétence en cybersécurité devrait être incluse dans la prochaine mise à jour de leur programme par le ministère de l'Éducation ou le ministère de l'Enseignement supérieur.

Figure 7 – Niveau d'accord, par ordre d'enseignement, avec l'idée d'inclure l'acquisition d'une compétence reliée à la cybersécurité dans le devis ministériel



Question : *« Veuillez indiquer votre niveau d'accord avec l'énoncé suivant : la prochaine mise à jour de ce programme par le ministère de l'Éducation et de l'Enseignement supérieur devrait inclure l'acquisition d'une compétence reliée à la cybersécurité. »*

Cette enquête portant sur la perception des établissements d'enseignement quant à l'importance de la cybersécurité en formation minière a donc permis de mieux comprendre comment les établissements d'enseignement offrant les programmes de formation et d'études menant à l'exercice des métiers et des professions les plus recherchés dans le secteur minier du Québec conçoivent la cybersécurité ainsi que l'importance pour les personnes apprenantes inscrites dans ces programmes d'accroître leurs compétences en cette matière. Les résultats

collectés montrent que l'ensemble des établissements d'enseignement sondés considèrent que la cybersécurité représente un enjeu important pour le secteur minier et cela s'illustre notamment par le fait que plus des trois quarts des personnes répondantes estiment « Très probable » ou « Assez probable » que soient instaurées au cours des deux prochaines années une ou plusieurs activités pédagogiques visant à sensibiliser les personnes apprenantes à la cybersécurité dans le programme offert par leur établissement d'enseignement. Tant en formation professionnelle que collégiale, la majorité des répondantes et des répondants considèrent que les personnes apprenantes doivent développer des compétences en cybersécurité pour occuper des postes dans le secteur minier. L'opinion des personnes répondantes provenant des deux ordres d'enseignement diverge cependant en ce qui a trait au niveau des compétences en cybersécurité devant être possédée, car alors que les personnes répondantes de la formation professionnelle évaluent qu'un niveau « de base » en cette matière est nécessaire, les personnes répondantes en formation collégiale jugent quant à elles qu'un niveau « intermédiaire » est nécessaire pour occuper des postes dans le domaine des mines. Cette différence de point de vue entre les personnes répondantes des deux ordres d'enseignement n'empêche cependant pas tant la formation professionnelle que collégiale d'être plutôt favorable à l'idée d'inclure l'acquisition d'une compétence reliée à la cybersécurité dans les devis ministériels de leurs programmes de formation minière.

Discussions, recommandations et limites

Dans le cadre de ce rapport de stage, nous avons cherché à mieux déterminer la place accordée à la cybersécurité dans la formation minière dispensée dans les établissements d'enseignement du Québec. Les résultats obtenus ont tout d'abord permis de mettre en lumière le niveau de sensibilisation aux action-clés relatives à la cybersécurité dans les programmes de formation minière analysés. Les données montrent à cet égard la présence d'un certain degré de sensibilisation à la cybersécurité, bien que cette sensibilisation reste toutefois limitée. Ce constat doit cependant être mis de l'avant avec précaution, car la taille réduite de l'échantillon a pu induire un effet de tendance centrale. En conservant cette précaution à l'esprit, il est possible de constater que ce soit en ce qui concerne l'action-clé « Utiliser adéquatement et en toute sécurité les équipements numériques », l'action-clé « Protéger les données personnelles et corporatives » ou encore l'action-clé « Gérer les risques », une majorité de personnes répondantes soulignent être « Peu » ou « Pas du tout » en accord avec l'énoncé selon lequel les personnes apprenantes y sont sensibilisées. Les résultats montrent également que les établissements d'enseignement offrant les programmes de formation minière les plus recherchés par l'industrie offrent peu de sensibilisation en dehors de celle destinée à rehausser la maîtrise des trois l'actions-clés identifiées, et ce, comme l'expose le fait qu'un seul programme offert dans un établissement d'enseignement collégial indique avoir instauré d'autres activités de sensibilisation à la cybersécurité que celles visant le développement des trois l'actions-clés retenues pour structurer cette enquête.

Par la suite, les résultats ont illustré la perception des programmes de formation et d'études analysés à l'égard de la cybersécurité dans le secteur minier et de l'importance des compétences en cybersécurité dans les programmes les plus en demande au sein de l'industrie minière. Les données colligées montrent que les personnes répondantes des établissements d'enseignement offrant la formation minière la plus recherchée par le secteur minéral sont conscients de l'importance que revêt la cybersécurité dans cette industrie en 2020. Elles sont par conséquent une majorité à considérer qu'il est nécessaire que les personnes apprenantes se destinant à travailler dans le secteur minier développent des compétences en cybersécurité,

bien que le niveau de compétence requis ne fasse pas l'objet d'un consensus parmi les ordres d'enseignement. Enfin, l'idée d'inclure une compétence en cybersécurité dans le devis ministériel des programmes de formation analysés recueille une majorité d'avis favorables parmi les personnes répondantes.

Ces multiples résultats obtenus grâce à la collecte de données peuvent être croisés avec les travaux de certains auteurs sur le sujet. Dans un premier temps, il est possible de constater que la sensibilisation de la main-d'œuvre aux menaces découlant des cyberrisques est primordiale pour que celle-ci soit pleinement consciente de l'importance de respecter tant les mesures de cyberhygiène que les politiques de cybersécurité mises en place par les entreprises (Li et al., 2019, p. 16; Soomro et al., 2016, p. 219). La collecte de données réalisée dans le cadre de ce rapport démontre qu'en matière de sensibilisation, les actions-clés « Utiliser adéquatement et en toute sécurité les équipements numériques », « Protéger les données personnelles et corporatives » et « Gérer les risques » sont respectivement l'objet d'une sensibilisation dans une minorité de programmes de formation minière professionnelle et collégiale. Par conséquent, il est possible de postuler qu'en ce qui concerne la formation initiale offerte à la main-d'œuvre minière, la sensibilisation à la cybersécurité est insuffisante dans une majorité de programmes, ce qui ne favorise pas l'émergence d'une prise de conscience de l'importance de la cybersécurité et des mesures de cyberhygiène chez la relève du secteur des mines.

La littérature portant sur la cybersécurité souligne également qu'en ce qui a trait aux mesures qu'une organisation peut mettre en place pour rehausser sa cybersécurité, le fait d'offrir de la formation à sa main-d'œuvre représente l'une des composantes les plus efficaces à mettre en place (Ma et al., 2009, p. 66). Dans le cadre d'un programme de sécurité informatique, la mise en place d'une offre de formation améliore en effet la prise de conscience relativement aux cyberrisques, la compréhension des enjeux en cette matière et donc la participation active du personnel aux programmes de cybersécurité (Ma et al., 2009, p. 66). Les données recueillis permettent de constater qu'il est nécessaire pour les personnes apprenantes inscrites en formation minière dans les programmes de formation professionnelle et collégiale les plus en demande dans le secteur minier du Québec de développer des compétences en

cybersécurité pour occuper des postes dans le secteur minier. C'est pourquoi, bien que la sensibilisation relativement aux trois actions-clés en cybersécurité requises à l'ère du numérique dans le secteur minier demeure limitée, plus des trois quarts des établissements d'enseignement répondants estiment qu'il est probable qu'une activité pédagogique de sensibilisation à la cybersécurité soit incluse dans la formation offerte aux personnes apprenantes d'ici 2022.

Pistes de recherches futures

En s'appuyant sur les données collectées et analysées, il est possible d'entrevoir plusieurs recherches supplémentaires qui pourraient être menées afin d'établir un portrait encore plus documenté de la cybersécurité dans la formation minière au Québec. Pour ce faire, trois pistes de recherche additionnelles semblent particulièrement prometteuses.

D'abord, la réalisation d'une recherche de même nature que celle menée dans ce rapport, mais s'adressant aux programmes universitaires les plus recherchés dans l'industrie minière du Québec, représenterait une piste de recherche pertinente pour le futur. En effet, puisque le présent rapport s'est concentré sur les programmes de formation professionnelle et de formation collégiale, la réalisation d'un tel exercice permettrait d'obtenir un portrait de la cybersécurité en formation minière couvrant les ordres d'enseignement professionnel, collégial et universitaire.

Ensuite, la comparaison entre la sensibilisation à la cybersécurité recensée dans le présent rapport et la sensibilisation à la cybersécurité instaurée dans la formation minière offerte dans d'autres États à l'échelle internationale pourrait également représenter une piste de recherche intéressante pour mettre à profit les données collectées dans le cadre du présent rapport. Une telle analyse comparative aurait la vertu de positionner le Québec à l'échelle internationale tout en permettant d'en apprendre davantage sur les meilleures pratiques de sensibilisation à la cybersécurité en formation minière.

Finalement, une autre piste de recherche porteuse afin de pousser plus loin la réflexion en matière de cybersécurité en formation minière consisterait à analyser la formation relative à

la cybersécurité qu'offre par les entreprises minières à leur personnel ainsi que les besoins de ces mêmes entreprises en matière de compétences en cybersécurité. La réalisation d'un projet de ce type permettrait de disposer d'un portrait de la formation continue complémentaire au portrait de la formation initiale dressé dans le présent rapport. De plus, la recension des besoins des entreprises minières en matière de compétences en cybersécurité permettrait de vérifier si la sensibilisation aux compétences en cybersécurité dans les programmes de formation analysés dans le présent rapport répond aux attentes de l'industrie.

Limites de la recherche

Cette recherche comporte quelques limites qui doivent être prises en considération. D'abord, le questionnaire est principalement constitué de questions comportant des échelles de mesure en cinq points. Le recours à ce type d'échelle de mesure peut comporter certaines limites. Parmi ces limites, il est possible de citer le fait que cette échelle de mesure induit parfois un effet de tendance centrale, ce qui peut avoir influencé les résultats obtenus. De plus, la taille de l'échantillon représente une autre limite à prendre en compte. En effet, seulement dix-sept personnes ont répondu au questionnaire. Cette faible quantité de personnes répondantes fait en sorte qu'il est nécessaire de garder une réserve en ce qui a trait à la généralisation des résultats.

Conclusion

En conclusion, le mandat confié au stagiaire par le mandant dans le cadre de ce stage consistait à élaborer un rapport documentant la place de la cybersécurité dans les cursus scolaires menant à l'exercice d'un métier ou d'une profession du secteur minier à l'ère du numérique. Pour ce faire, nous avons d'abord analysé la place accordée à la cybersécurité dans la formation minière dispensée dans les établissements d'enseignement du Québec offrant de la formation minière, puis nous avons examiné la perception de ces établissements à l'égard de la cybersécurité en formation minière.

Les résultats obtenus démontrent que l'amélioration des compétences en cybersécurité de la main-d'œuvre du secteur minier constitue un impératif dans un secteur minéral qui se caractérise aujourd'hui par une numérisation accrue et un degré d'interconnectivité sans précédent. En ce qui a trait à la sensibilisation des personnes apprenantes aux trois actions-clés en cybersécurité nécessaires à maîtriser dans les mines à l'ère numérique, le rapport témoigne d'une situation contrastée où certaines formes de sensibilisation sont présentes dans une minorité des programmes analysés, mais où toutefois la majeure partie des programmes n'offrent pas de sensibilisation. L'utilisation d'une échelle de mesure en cinq points pour collecter les données pourrait entre autres expliquer ce contraste.

La perception des personnes répondantes des programmes de formation professionnelle et d'études collégiales en formation minière à l'égard de la cybersécurité est fort probablement mieux définie grâce à ce rapport. En effet, nous savons désormais que les personnes répondantes des programmes de formation analysés considèrent que le secteur minier doit accorder de l'importance à la cybersécurité dans le cadre de ses activités et que par conséquent, le développement de compétences en cybersécurité est nécessaire chez les personnes apprenantes désirant travailler dans le domaine des mines. Cette collecte de données a également été l'occasion de constater que les personnes répondantes des programmes de formation analysés perçoivent dans leur majorité que les personnes apprenantes qui désirent travailler dans le secteur minier doivent posséder des compétences de niveau intermédiaire ou de base en cybersécurité afin d'œuvrer dans le secteur minier. De

plus, la majorité des personnes répondantes se positionnent favorablement par rapport à l'idée d'inclure une compétence en cybersécurité dans les devis ministériels.

En améliorant la connaissance à propos de la cybersécurité en formation minière, ce rapport de stage a permis de faire progresser non seulement notre compréhension de l'état actuel de la formation menant vers l'exercice d'un métier ou d'une profession du secteur minier québécois, mais également d'ouvrir de nouvelles perspectives de recherche porteuse pour le futur de l'éducation au Québec. Au niveau professionnel, la réalisation de ce rapport de stage marque une autre étape dans la poursuite de notre intégration dans notre milieu de travail.

Bibliographie

Austmine (2018). *Cyber security in mining operations*, [En ligne], 15 p., http://www.austmine.com.au/Publications/category/publications/cyber-security-in-mining-operations-ebook (Page consultée le 18 septembre 2020).

Baylon, Caroline (2014). *Challenges at the Intersection of Cyber Security and Space Security : Country and International Institution Perspectives*, [En ligne], Londres, Royal Institute of International Affairs, 51 p., https://www.chathamhouse.org/2014/12/challenges-intersection-cyber-security-and-space-security-country-and-international (Page consultée le 1er octobre 2020).

CDW Canada (2020). *Cyber Resilience : An Evolving Perspective*, [En ligne], 87 p., https://fr.cdw.ca/content/cdwca/en/solutions/cybersecurity/security-study.html (Page consultée le 18 septembre 2020).

CISCO (Page consultée le 8 octobre 2020). *What Is Cybersecurity?*, [En ligne], https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Comité sectoriel de main-d'œuvre de l'industrie des mines (2020). *Estimation des besoins de main-d'oeuvre du secteur minier au Québec : 2019-2023 avec tendances 2028*, [En ligne], 52 p., https://www.explorelesmines.com/images/pdf/Section_corporative/Publications/Etudes_sectorielles/EBMO_final.pdf (Page consulté le 23 octobre 2020).

Deloitte (2018). *An integrated approach to combat cyber risk Securing industrial operations in mining*, [En ligne], 21 p., https://www2.deloitte.com/global/en/pages/energy-and-resources/articles/approach-to-combat-cyber-risk-mining.html (Page consultée le 2 septembre 2020).

Ernst & Young et associés (2018). *Does cyber risk only become a priority once you've been attacked ? : Mining and metals*, [En ligne], 8 p., https://www.ey.com/Publication/vwLUAssets/ey-cyber-in-mining-report/$File/EY-cyber-in-mining-report.pdf (Page consultée le 2 septembre 2019).

Forum économique mondial (2017). *Digital Transformation Initiative Mining and Metals Industry*, [En ligne], 35 p., http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/wef-dti-mining-and-metals-white-paper.pdf (Page consultée le 21 août 2020).

Inmarsat (2020). *The Rise of IoT in Mining*, [En ligne], 31 p., https://research.inmarsat.com/2020/download-report/ (Page consultée le 10 juillet 2020).

Institut de la statistique du Québec (2019). *Mines en chiffres—L'investissement minier au Québec en 2018*, [En ligne], 11 p., https://bdso.gouv.qc.ca/docs-ken/multimedia/PB01633FR_mine2018H00F00.pdf (Page consultée le 12 août 2020).

Institut de la statistique du Québec (2020). *Mines en chiffres—La production minérale au Québec en 2018*, [En ligne], 13 p., https://statistique.quebec.ca/fr/fichier/mines-en-chiffres-production-minerale-quebec-2018.pdf (Page consultée le 12 août 2020).

Institut national des mines (2018a). *Les tendances générales en formation minière en 2018*, [En ligne], 24 p., https://inmq.qc.ca/medias/files/Publications/Rapports_de_recherche/INMQ_Tendances_generales_formation_miniere_11_janv_28juin2018.pdf (Page consultée le 17 août 2020).

Institut national des mines (2020). *Plan stratégique 2018-2023*, [En ligne], 28 p., https://inmq.qc.ca/medias/files/Documents_officiels/PlanificationStrategique_revisee_2020.pdf (Page consulté le 2 décembre 2020).

Institut national des mines (2018b). *Transformation numérique et compétences du 21e siècle pour la prospérité du Québec - Exemple de l'industrie minière*, [En ligne], 72 p., https://inmq.qc.ca/medias/files/Publications/Rapports_de_recherche/INMQ_Transformation_numerique_complet.pdf (Page consultée le 12 août 2020).

Institut national des mines, Comité sectoriel de main-d'œuvre de l'industrie des mines et Association minière du Québec (2020). *Le cadre de référence des compétences à l'ère du numérique dans le secteur minier*, [En ligne], 18 p.,

https://inmq.qc.ca/medias/files/Publications/Rapports_de_recherche/Cadre_references_metiers/INMQ_Cadre_reference_competence_ere_numerique.pdf (Page consultée le 12 août 2020).

Kohler, Dorothée, et Jean-Daniel Weisz (2016). « Industrie 4.0 : Comment caractériser cette quatrième révolution industrielle et ses enjeux? », *Annales des Mines - Réalités industrielles*, novembre 2016, no 4, p. 51-56.

Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar et Xiaohong Yuan (2019). « Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior », *International Journal of Information Management*, vol. 45, p. 13-24.

Loi sur l'Institut national des mines. RLRQ, c. I-13.1.2, http://www.legisquebec.gouv.qc.ca/fr/ShowDoc/cs/I-13.1.2

Ma, Qingxiong, Mark Schmidt et Michael Pearson (2009). « An Integrated Framework for Information Security Management », *Review of Business*, vol. 30, no. 1, p. 58-69.

Marsh (2018) *Cyber Risk : Threats and Insurance Protection for the Mining Sector*, [En ligne], 14 p., https://www.marsh.com/uk/insights/research/cyber-risk-threats-and-insurance-protection-for-the-mining-sector.html (Page consultée le 8 septembre 2020).

Marsh et Microsoft (2019). *2019 Global Cyber Risk Perception Survey*, [En ligne], 34 p., https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf (Page consultée le 8 septembre 2020).

Ministère de l'Économie et de l'Innovation (2016). « Industrie 4.0 : Les défis de la quatrième révolution industrielle », dans *Bulletin Espace Conseils PME*, [En ligne], https://www.economie.gouv.qc.ca/bibliotheques/outils/gestion-dune-entreprise/industrie-40/industrie-40-les-defis-de-la-quatrieme-revolution-industrielle/

Ministère de l'Économie et de l'Innovation (2018). « L'industrie 4.0 – L'humain au cœur de la transformation numérique », dans *Bulletin Espace Conseils PME*, [En ligne], https://www.economie.gouv.qc.ca/bibliotheques/outils/gestion-dune-entreprise/industrie-40/lindustrie-40-lhumain-au-coeur-de-la-transformation-numerique/

Ministère de l'Économie et de l'Innovation (2019). « Internet des objets », le ministère, [En ligne], https://www.economie.gouv.qc.ca/bibliotheques/sous-secteur/logiciel/internet-des-objets/

Ministère de l'Éducation et de l'Enseignement supérieur (2019). *Cadre de référence de la compétence numérique*, [En ligne], Québec, le ministère, 34 p., http://www.education.gouv.qc.ca/fileadmin/site_web/documents/ministere/Cadre-reference-competence-num.pdf (Page consultée le 5 août 2020).

NOVIPRO et Léger (2020). *Portrait des TI dans les moyennes et grandes entreprises canadiennes*, [En ligne], Montréal, NOVIPRO, 38 p., https://cdn2.hubspot.net/hubfs/2715025/Étude%20TI%202020/Portrait_des_TI_2020_NOVIPRO_LEGER.pdf?utm_campaign=%C3%89tudeTI%202020&utm_source=hs_automation&utm_medium=email&utm_content=82452705&_hsenc=p2ANqtz-9f9oUowmBlbIZC-YIabeyEaiJE8enfiGBnDvEV-ztCKyDeal3sGmFLidm3Wq6kpWnaq7XKQ_2QvfSkU1QMEz799XlfCVzZyuqz-eGwkPfPyXrGws8&_hsmi=82452705 (Page consultée le 14 octobre 2020).

PricewaterhouseCoopers (2020a). *23rd Annual Global CEO Survey : Navigating the rising tide of uncertainty*, [En ligne], 49 p., https://www.pwc.com/gx/en/ceo-survey/2020/reports/pwc-23rd-global-ceo-survey.pdf (Page consultée le 8 octobre 2020).

PricewaterhouseCoopers (2020b). *Mines 2020 - Minières canadiennes : Ingéniosité et résilience*, [En ligne], https://www.pwc.com/ca/fr/industries/mining/mine-2020.html (Page consultée le 8 octobre 2020).

RSA Security (2016). *Cyber Risk Appetite : Defining and Understanding Risk in the Modern Enterprise*, [En ligne], 4 p., https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf (Page consultée le 14 octobre 2020).

Schatz, Daniel, Rabih Bashroush et Julie Wall (2017). « Towards a More Representative Definition of Cyber Security », *Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, p. 53-74.

Secrétariat du Conseil du trésor (2020). *Politique gouvernementale de cybersécurité*, [En ligne], Québec, le ministère, 12 p., https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/SCT/vitrine_numeriQc/cybersecurite/politique-gouvernementale-cybersecurite.pdf?1603474893 (Page consultée le 8 septembre 2020).

Sécurité publique Canada (2018). *Stratégie nationale de cybersécurité : Vision du canada pour la sécurité et la prospérité dans l'ère numérique*, [En ligne], Ottawa, le ministère, 39 p., https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx (Page consultée le 8 septembre 2020).

Soomro, Zahoor A., Mahmood H. Shah et Javed Ahmed (2016). « Information security management needs more holistic approach : A literature review », *International Journal of Information Management*, vol. 36, p. 215-225.

Willis Towers Watson (2017). *From technology to people : The new frontier in mining cyber risk*, [En ligne], 6 p., https://www.willistowerswatson.com/en/insights/2017/09/mining-risk-review-from-technology-to-people-the-new-frontier-in-mining-cyber-risk (Page consultée le 3 août 2020).

Annexe I

Questionnaire utilisé pour collecter les données auprès des établissements d'enseignement

Sondage sur la cybersécurité - Profil de la répondante ou du répondant

* 1. Quel est le nom de votre établissement d'enseignement?

* 2. Quelle est votre fonction?

Enseignante ou enseignant

Professionnelle ou professionnel

Personnel de soutien

Personnel d'encadrement

Autre (veuillez préciser)

* 3. Quel est le nom du programme d'études ou de formation pour lequel vous répondez à ce questionnaire?

DEC en technologie minérale-spécialisation en géologie

DEC en technologie minérale-spécialisation en exploitation

DEC en technologie de l'électronique industrielle

DEP en conduite de machinerie lourde en voirie forestière

DEP en extraction de minerai

DEP en mécanique d'engins de chantier

Sondage sur la cybersécurité – Définition

* 4. Selon vous, à quoi renvoie la notion de cybersécurité?

L'ensemble des solutions technologiques mobilisées pour protéger un réseau.

La mise en place d'un pare-feu sur votre ordinateur.

La sécurisation des mots de passe sur un réseau ou sur internet.

La protection des infrastructures et des informations numériques.

L'isolation d'un système d'information d'un virus informatique.

Autre (veuillez préciser)

Sondage sur la cybersécurité - Acquisition des compétences en cybersécurité

Dans le cadre de ce questionnaire, le concept de « cybersécurité » doit être interprété au sens large, comme englobant toutes les pratiques permettant d'améliorer la protection des informations numériques et des infrastructures sur lesquelles elles reposent (systèmes, réseaux, programmes, etc.) contre les attaques numériques.

* 5. Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : dans le cadre du programme d'études actuellement en vigueur, les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques (Exemple : Gestion des mots de passe).

Tout à fait en accord

Assez en accord

Peu en accord

Pas du tout en accord

Je ne sais pas

6. Le cas échéant, veuillez spécifier la ou les activité(s) pédagogique(s) de sensibilisation effectuée(s) ainsi que leurs objectifs.

* 7. Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : Dans le cadre du programme d'études actuellement en vigueur, les personnes apprenantes sont sensibilisées à

l’importance d’appliquer les lois et les politiques relatives à la protection des informations personnelles ou de l’entreprise.

Tout à fait en accord

Assez en accord

Peu en accord

Pas du tout en accord

Je ne sais pas

8. Le cas échéant, veuillez spécifier la ou les activité(s) pédagogique(s) de sensibilisation effectuée(s) ainsi que leurs objectifs.

* 9. Dans quelle mesure êtes-vous en accord avec l'affirmation suivante : dans le cadre du programme d’études actuellement en vigueur, les personnes apprenantes sont sensibilisées à la gestion des risques numériques notamment par l’identification des événements pouvant avoir un impact sur le travail (Exemple : Identifier et rapporter les incidents de cybersécurité, reconnaître un courriel d’hameçonnage, etc.).

Tout à fait en accord

Assez en accord

Peu en accord

Pas du tout en accord

Je ne sais pas

10. Le cas échéant, veuillez spécifier la ou les activité(s) pédagogique(s) de sensibilisation effectuée(s) ainsi que leurs objectifs.

* 11. Avez-vous, dans le cadre du programme d’études actuellement en vigueur, instauré toute autre activité ayant pour but la sensibilisation à toute notion relative à la cybersécurité?

Oui

Non

12. Si vous avez répondu « Oui » à la question précédente, veuillez spécifier la ou les activité(s) de sensibilisation effectuée(s) ainsi que leurs objectifs.

* 13. Au cours des 2 prochaines années, est-il probable que soient instaurées une ou plusieurs activités pédagogiques visant à sensibiliser les personnes apprenantes à la cybersécurité dans le cadre du programme d'études actuellement en vigueur?

Très probable

Assez probable

Peu probable

Très peu probable

Pas du tout probable

Sondage sur la cybersécurité - Perception de l'importance de la cybersécurité

* 14. Selon vous, quel niveau d'importance le secteur minier doit-il accorder à la cybersécurité dans ses activités?

Très important

Assez important

Peu important

Très peu important

Pas du tout important

* 15. Selon vous, est-il nécessaire aux personnes apprenantes actuellement inscrites à ce programme de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier?

Très nécessaire

Assez nécessaire

Peu nécessaire

Très peu nécessaire

Pas du tout nécessaire

Je ne sais pas

* 16. Selon vous, quel niveau de compétence en cybersécurité devrait posséder les personnes apprenantes inscrites à ce programme pour occuper des postes dans le secteur minier?

Niveau expert

Niveau avancé

Niveau intermédiaire

Niveau de base

Aucun niveau

* 17. Veuillez indiquer votre niveau d'accord avec l'énoncé suivant : la prochaine mise à jour de ce programme par le ministère de l'Éducation et de l'Enseignement supérieur devrait inclure l'acquisition d'une compétence reliée à la cybersécurité.

Tout à fait en accord

Assez en accord

Peu en accord

Très peu en accord

Pas du tout en accord

Autre (veuillez préciser)

* 18. Dans le cadre de votre fonction actuelle, avez-vous déjà suivi une formation en lien avec la cybersécurité?

Oui

Non

Autre (veuillez préciser)

* 19. Quel est votre niveau d'intérêt à suivre une formation relative à la cybersécurité?

Très intéressé(e)

Assez intéressé(e)

Peu intéressé(e)

Très peu intéressé(e)

Pas du tout intéressé(e)

* 20 Veuillez préciser pour quelles raisons vous avez ce niveau d'intérêt.

Sondage sur la cybersécurité - Commentaires

* 21 Avez-vous un commentaire ou des suggestions