Portrait de la cybersécurité

dans les programmes de formation professionnelle et les programmes d'études collégiales

menant à l'exercice d'un métier ou d'une profession dans le secteur minier au Québec

Institut national des mines
Québec

Recherche, analyse et rédaction
Nicholas Théroux, conseiller à l'innovation et à la recherche
Institut national des mines

Supervision
Jean-François Pressé, président-directeur général
Institut national des mines

Diffusion
Karine Lacroix, conseillère en communication
Institut national des mines

Révision linguistique
Syn-Texte

Graphisme
Pro-Actif

Photographie
Les photographies présentes dans cette publication ont été prises avant mars 2020.

(page couverture) Une étudiante en Technologie minérale du Cégep de Thetford effectue un essai de compression d'une éprouvette de roche. (Photographe : Mélodie Roy)

Le présent ouvrage a été produit par l'Institut national des mines.

Comment citer cet ouvrage :
Québec. Institut national des mines (2021). *Portrait de la cybersécurité dans les programmes de formation professionnelle et les programmes d'études collégiales menant à l'exercice d'un métier ou d'une profession dans le secteur minier au Québec*, Études et rapports, Rédigé par Nicholas Théroux, Val-d'Or, 60 p.

Pour toute demande de renseignement :
Institut national des mines
125, rue Self
Val-d'Or (Québec) J9P 3N2

Téléphone : 819 825-4667
info@inmq.gouv.qc.ca | inmq.gouv.qc.ca

ISBN : 978-2-550-89052-2 (Imprimé)
ISBN : 978-2-550-89053-9 (PDF)

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2021

AVANT-PROPOS

L'un des axes du plan stratégique 2018-2023 de l'Institut national des mines énonce que l'organisme doit documenter, grâce à des activités de veille, les tendances innovantes en formation minière à l'échelle mondiale. Depuis 2018, cette veille informationnelle de l'Institut a fait ressortir toute l'importance que revêt l'acquisition de compétences en cybersécurité pour la main-d'œuvre appelée à travailler dans l'industrie minière au 21e siècle (Institut national des mines, 2018a). Dans ce document, l'Institut présente un portrait de la formation en cybersécurité dans les établissements d'enseignement du Québec qui offrent de la formation menant à l'exercice d'un métier ou d'une profession du secteur minier.

Le *Portrait de la cybersécurité dans les programmes d'études québécois menant à l'exercice d'un métier ou d'une profession dans le secteur minier* n'aurait pas vu le jour sans la collaboration des établissements d'enseignement du Québec qui offrent de la formation minière. L'Institut tient à les remercier de leur collaboration.

TABLE DES MATIÈRES

LISTE DES TABLEAUX ET DES FIGURES

Liste des tableaux

Liste des figures

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 pour 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 un cyberenvironnement et à ses utilisateurs (notre traduction)[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].

Résilience

Capacité des systèmes à résister ou à se relever en cas d'incident[1].

1 Définition provenant 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 (Ministère de l'Économie et de l'Innovation, 2019).

RÉSUMÉ

Depuis 2018, la veille informationnelle hebdomadaire réalisée par l'Institut national des mines témoigne de l'importance majeure qu'occupent les enjeux liés à la cybersécurité pour l'industrie minière dans le contexte où s'intensifie sa transformation numérique. La numérisation accrue des outils de travail ainsi que la connectivité croissante des équipements industriels constituent autant d'éléments qui font en sorte que l'acquisition de compétences en cybersécurité représente un incontournable pour la main-d'œuvre du secteur minier au 21e siècle.

Dans ce rapport, l'Institut a documenté la place accordée à la cybersécurité dans les programmes de formation minière les plus recherchés au Québec ainsi que la perception des établissements d'enseignement qui offrent ces formations à l'égard de la cybersécurité en formation minière.

Les résultats recueillis démontrent que la sensibilisation des personnes apprenantes en formation minière à des compétences en cybersécurité qui sont requises à l'ère du numérique dans les mines demeure limitée. En effet, aucune des compétences ne fait l'objet d'une sensibilisation dans la majorité des programmes de formation professionnelle et collégiale analysés. Toutefois, l'ensemble des personnes répondantes des programmes 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 les compétences en cybersécurité qui sont nécessaires pour travailler dans le secteur minier actuellement sont de niveau de base et intermédiaire. La majorité des personnes répondantes indiquent par conséquent être favorables à l'idée d'inclure l'acquisition d'une compétence en cybersécurité dans les devis ministériels qui encadrent les programmes de formation minière.

Les données colligées par cette recherche illustrent le fait que les établissements d'enseignement du Québec qui offrent de la formation minière conçoivent bien l'importance de transmettre à leurs personnes apprenantes des compétences en cybersécurité. Cependant, les initiatives mises en œuvre à cet égard sont plutôt restreintes et 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, la venue 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, la main-d'œuvre du secteur minier doit développer ses compétences numériques en vue 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 de l'Enseignement supérieur (MEES), qui énonce, dans le *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 d'elles étant constituée de plusieurs éléments, c'est-à-dire des habiletés associées à la maîtrise de la dimension (Ministère de l'Éducation et de l'Enseignement supérieur, 2019, p. 11). Le *Cadre de référence de la compétence numérique* a permis au Ministère de déterminer que la dimension *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). Au cœur des éléments nécessaires à la maîtrise de cette dimension figure l'aptitude à « sécuriser ses 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* aux compétences de la main-d'œuvre au 21e siècle en matière de cybersécurité concorde avec les constats de l'Institut, qui depuis 2018, effectue une veille informationnelle chaque semaine. Cela lui a permis de repérer la question du cyberrisque, qui 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 que jusqu'à ce jour la cybersécurité représente l'une des priorités majeures de l'industrie minière contemporaine.

Ce souci particulier à l'égard de cette problématique découle notamment du fait qu'avec le développement rapide de l'Internet des objets au sein de l'industrie minière, le risque de cyberattaques ne cesse de s'accroître, puisque 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 à l'égard de 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 qui peuvent 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 leur exploitation (Inmarsat, 2020). Dans un rapport de 2017, le cabinet de conseil Willis Towers Watson soulignait de son côté que la vaste majorité des entreprises qui investissent dans le but 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 pour faire face efficacement à l'enjeu de la cybersécurité qui est de plus en plus incontournable à l'ère de la quatrième révolution industrielle ?

Objectifs du rapport

Par ce rapport, l'Institut 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 en formation minière. De plus, grâce à une revue de littérature portant sur l'importance de la cybersécurité dans le secteur minier à l'ère de l'industrie 4.0, ce rapport permet de réfléchir à la place qu'occupe la cybersécurité dans le curriculum menant à l'exercice d'un métier ou d'une profession du secteur minier.

Plan sommaire

Ce rapport s'articule en cinq chapitres. Tout d'abord, le premier chapitre détaille la méthodologie utilisée pour collecter les données nécessaires à cette recherche. Après une mise en contexte des innovations qui caractérisent la mine intelligente actuelle et future et qui expose le lien entre l'industrie minière 4.0 et la cybersécurité, le deuxième chapitre présente une revue de littérature détaillant l'importance des compétences en cybersécurité dans l'industrie minière à l'ère de la quatrième révolution industrielle et de la mine intelligente. Suit le troisième chapitre, qui présente un état de la situation concernant la sensibilisation aux compétences relatives à la cybersécurité dans la formation minière québécoise. De plus, la perception des établissements d'enseignement du Québec qui offrent de la formation minière en ce qui a trait à la cybersécurité dans le curriculum menant à l'exercice d'un métier ou d'une profession du secteur minier est étudiée. Le quatrième chapitre, quant à lui, permet d'analyser l'état de la situation qui nous est présentée. Finalement, le cinquième chapitre présente des pistes de recherche susceptibles de favoriser le développement des compétences en cybersécurité dans la formation minière québécoise.

Les équipements miniers génèrent de plus en plus de données. Le personnel de la mine Canadian Malartic veille à assurer la gestion et la sécurité de ses données dans ses opérations quotidiennes. (Photographe : Mathieu Dupuis)

1. MÉTHODOLOGIE ET ÉCHANTILLONNAGE

La méthodologie utilisée pour produire ce rapport s'appuie sur une approche à la fois qualitative et 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 a été menée à l'aide d'un questionnaire abordant deux grandes questions : d'abord, l'Institut a cherché à savoir si les personnes apprenantes étaient sensibilisées ou non aux compétences relatives à la cybersécurité dans les programmes de formation minière au Québec; ensuite, il s'est attardé à la perception des établissements d'enseignement à l'égard de la cybersécurité.

1.1 Méthodologie de la collecte de données

Le questionnaire[4] utilisé pour collecter les données a été élaboré au printemps 2020 par l'Institut. La plateforme de sondage en ligne *Survey Monkey* fut utilisée. Le questionnaire comptait 21 questions et le temps moyen de remplissage par les personnes répondantes était d'environ 10 minutes. Les établissements d'enseignement sélectionnés pour participer à la collecte de données ont été contactés pour 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 l'Institut pour 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.

1.2 Échantillonnage

Pour délimiter l'étendue de la recherche, il fut décidé que les trois programmes de formation professionnelle et les trois programmes d'études collégiales menant à l'exercice des métiers et des professions les plus recherchés dans le secteur minier du Québec seraient analysés dans le cadre de cette collecte de données. Cette décision découle du fait que 78 % des postes à pourvoir dans le secteur minier québécois à l'horizon de 2023 nécessiteront soit un diplôme d'études professionnelles (DEP), soit un diplôme d'études collégiales (DEC) (Comité sectoriel de main-d'œuvre de l'industrie des mines, 2020, p. 17).

4 Le questionnaire peut être consulté à l'**annexe I**.

Pour cibler les programmes de formation et les programmes d'études devant être analysés dans le cadre de cette collecte de données, l'Institut s'est basé sur l'étude *Estimation des besoins de main-d'œuvre du secteur minier au Québec 2019-2023 avec tendances 2028* (Comité sectoriel de la main-d'œuvre de l'industrie des 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 un ou plusieurs programmes de formation et d'études ciblés dans le rapport du comité sectoriel de la main-d'œuvre de l'industrie des mines ont été inclus dans la collecte de données[5].

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 la 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 pour ne centrer ce rapport que sur les formations menant à l'exercice d'un métier ou d'une profession directement en lien avec l'exploration minière, l'extraction du minerai ou le traitement de celui-ci. En ce qui concerne les métiers exigeant un DEC, 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 les centres de formation professionnelle présents dans 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, s'est donc substitué au DEP en conduite d'engins de chantier dans l'échantillon. Le **tableau 1** présente les établissements d'enseignement qui offrent les programmes de formation et les programmes d'études de cette collecte de données.

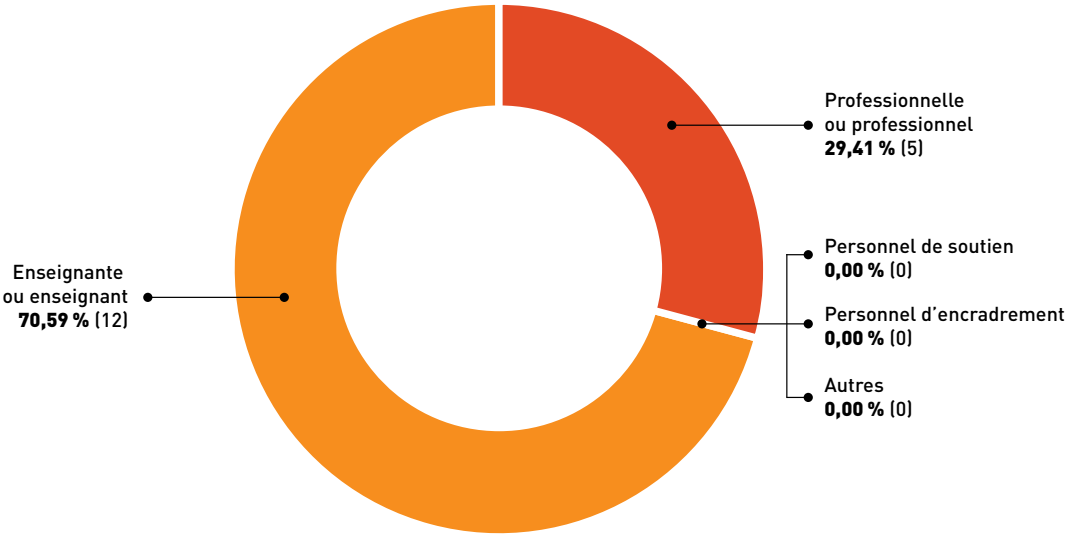
5 Selon l'Institut de la statistique du Québec, les trois principales régions minières du Québec sont le Nord-du-Québec, l'Abitibi-Témiscamingue et la Côte-Nord. Ces trois régions « fournissent la majorité des emplois dans le secteur minier, soit 63,8 % des emplois pour l'ensemble du Québec » et « se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

Tableau 1 **Établissements d'enseignement offrant les programmes de formation et les programmes sondés dans le cadre de la collecte de données**

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

La **figure 1** permet de constater que les personnes 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.

Figure 1 **Fonction occupée par les personnes répondantes dans les établissements d'enseignement**



Question : « Quelle est votre fonction ? »

L'ensemble des dix établissements d'enseignement sollicités pour remplir le questionnaire ont répondu favorablement à la demande de l'Institut, ce qui signifie que les six programmes analysés dans ce rapport ont obtenu les réponses de trois établissements d'enseignement différents, exception faite du programme *Extraction de minerai*, qui n'est offert que par deux établissements scolaires au Québec. Au total, dix-sept personnes répondantes ont 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 par l'Institut.

2. REVUE DE LITTÉRATURE LA CYBERSÉCURITÉ DANS LE SECTEUR MINIER À L'ÈRE DE LA 4e RÉVOLUTION INDUSTRIELLE

2.1 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 qui transforment radicalement les façons de faire. Le secteur minier n'échappe pas à ces processus, puisque les diverses technologies propres à l'industrie 4.0 y sont d'ores et déjà fermement implantées. Citons en exemple l'automatisation de certaines activités comme l'opération de véhicules de manière autonome ou télécommandée depuis un centre de contrôle qui peut se situer 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, 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 et Weisz, 2016).

L'effet de cette révolution industrielle sur l'industrie minière est incommensurable, d'autant plus que des innovations qui alimentent cette transformation ne cessent de se produire. Au stade où se situe actuellement la quatrième révolution industrielle, l'Institut estime que le concept de « mine intelligente » est celui qui permet le mieux de définir les retentissements de l'industrie 4.0 dans le secteur minier. Selon ce concept, les mines qui procèdent à leur transition vers l'industrie 4.0 deviennent « intelligentes », 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).

2.2 Les données et la connectivité : les éléments centraux de la quatrième révolution industrielle pour 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 décision et ainsi être utilisées à leurs pleines capacités, un complexe minier doit pouvoir compter sur une connectivité particulièrement fiable et à 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 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 accompli au moins un 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 liés à l'implantation de technologies de l'Internet des objets dans le secteur minier sont nombreux (Inmarsat, 2020). En effet, l'implantation de capteurs sur les multiples équipements d'un complexe minier permet de créer un véritable réseau d'appareils connectés, qui, lorsqu'ils sont connectés au système informatique de l'entreprise, donnent 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 en vue 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 commander et de surveiller à distance des équipements automatisés pour effectuer 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 témoignent d'ailleurs de la place centrale qu'occupe cette technologie dans la vision stratégique à long terme des entreprises minières pour leur permettre d'augmenter leur productivité, 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 qui ont précédé 2020; on prévoit que 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.

2.3 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 Associés mentionne que le degré élevé de connectivité qui caractérise désormais la technologie opérationnelle mise en œuvre dans les complexes miniers nécessite 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 faisaient face les entreprises minières était restreint, car une faible quantité d'équipement était connectée 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 considérablement augmenté les cyberrisques que peut encourir un complexe minier (Ernst & Young et Associés, 2018). L'interconnexion entre les systèmes et l'intégration entre les technologies de l'information (TI) ainsi que 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, et de compromettre 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).

2.3.1 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 pour les cyberrisques parmi les dix plus grandes entreprises 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 sociétés 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, puisque, 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 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 précèdent 2020 à 8,4 % pour les trois années qui suivent 2020 (Inmarsat, 2020).

Mais cette préoccupation vis-à-vis des enjeux liés à la cybersécurité n'est pas le propre du secteur minier, puisque de nombreuses études révèlent que les entreprises actives dans l'ensemble des secteurs d'activité 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'activité 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).

2.3.2 D'où provient 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. Le **tableau 2** synthétise les quatre grands groupes d'acteurs qui sont à même de représenter un cyberrisque pour les organisations.

Tableau 2 **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 qui peut conférer un avantage concurrentiel à ses propres activités minières. De plus, la réalisation d'une cyberattaque qui affecte la technologie opérationnelle 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 pour faire ralentir ou arrêter la production pour des motifs sociopolitiques ou environnementaux (Austmine, 2018).

Les entreprises concurrentes sont également désignées 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. 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 semble 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 de l'information sur la stratégie d'affaires d'une entreprise rivale qui pourront être utilisées pour mieux la concurrencer, mais elles sont également susceptibles d'être d'une grande utilité en prévision de négociations entre sociétés (Austmine, 2018; Deloitte, 2018).

Par ailleurs, la revue de littérature réalisée 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 qui agissent seuls ou en groupes n'épargnent aucun secteur d'activité, comme en témoigne la vague de cyberattaques qui ont ciblé plusieurs compagnies minières canadiennes entre 2013 et 2016 et qui se sont soldées par le vol de données personnelles et corporatives sensibles (Jenish, 2018).

Bien entendu, les acteurs malveillants externes ne représentent pas l'entièreté des individus ou des groupes qui font 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 de détecter que les acteurs internes représentent également une menace dont doivent tenir compte les entreprises du secteur minier (Deloitte, 2018). En effet, des employées ou des employés qui travaillent au sein 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 embauchée par une société minière dispose en effet d'une position privilégiée pour 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 dont l'effet sera de diminuer le niveau de cyberprotection de son organisation ou de porter atteinte à la sécurité des données dont elle dispose.

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

Les impacts pouvant découler d'une cyberattaque fructueuse sont multiples et leur niveau de gravité est variable. Le **tableau 3** synthétise les principales conséquences pouvant découler d'une cyberattaque qui a réussi à affecter les infrastructures opérationnelles d'un site minier. Les éléments qui y sont énumérés ne constituent cependant pas une liste exhaustive de toutes les conséquences possibles.

Tableau 3 **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
Incendies, explosions et autres dangers	Dommages aux équipements critiques	Perte d'occasions et de revenu
Perturbation des activités	Remise en question du permis social d'exploitation	Dégradation de l'image de marque et de la réputation

Source : Ernst & Young et Associés (2018)

Les conséquences d'une cyberattaque touchant les infrastructures opérationnelles d'une entreprise minière peuvent se révéler néfastes à plusieurs égards. D'abord, elle 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 incendies, des explosions ou d'autres dangers susceptibles non seulement de compromettre la sécurité du personnel, mais également de faire peser un risque sur l'environnement. Ensuite, elles peuvent aussi compromettre 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 certaine période. Finalement, des conséquences commerciales et réputationnelles sont prévisibles. En effet, le fait qu'une entreprise ait fait l'objet d'une cyberattaque fructueuse peut avoir une incidence sur son image et sa réputation tant auprès du grand public et des autorités publiques que des investisseurs. Par conséquent, des occasions 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 dans le **tableau 3** et dans les paragraphes précédents représentent les impacts possibles des cyberattaques qui réussissent à affecter les infrastructures opérationnelles d'une organisation. Les cyberattaques qui affectent uniquement les infrastructures informatiques d'une entreprise continuent également de représenter une grande menace pour les organisations de l'ensemble des secteurs, dont le secteur minier. Ce type de cyberattaque se caractérise généralement 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).

2.3.4 La cybersécurité : une responsabilité collective

La cybersécurité représente donc un enjeu majeur auquel est confronté le secteur minier à l'ère de la quatrième révolution industrielle. Il faut alors se demander comment l'industrie minière peut agir concrètement en vue de mettre en place des mesures efficaces en matière de cybersécurité ? Selon un rapport du cabinet de conseil Willis Towers Watson, au moins les deux tiers des cyberattaques fructueuses qui affectent les entreprises du secteur minier résultent d'un comportement inadéquat venant 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 l'École Polytechnique de 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 et 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, 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 et les applications sont en effet d'ores et déjà largement utilisés dans le secteur minier, et tout indique que leur utilisation continuera de 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 « [l]a 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.)

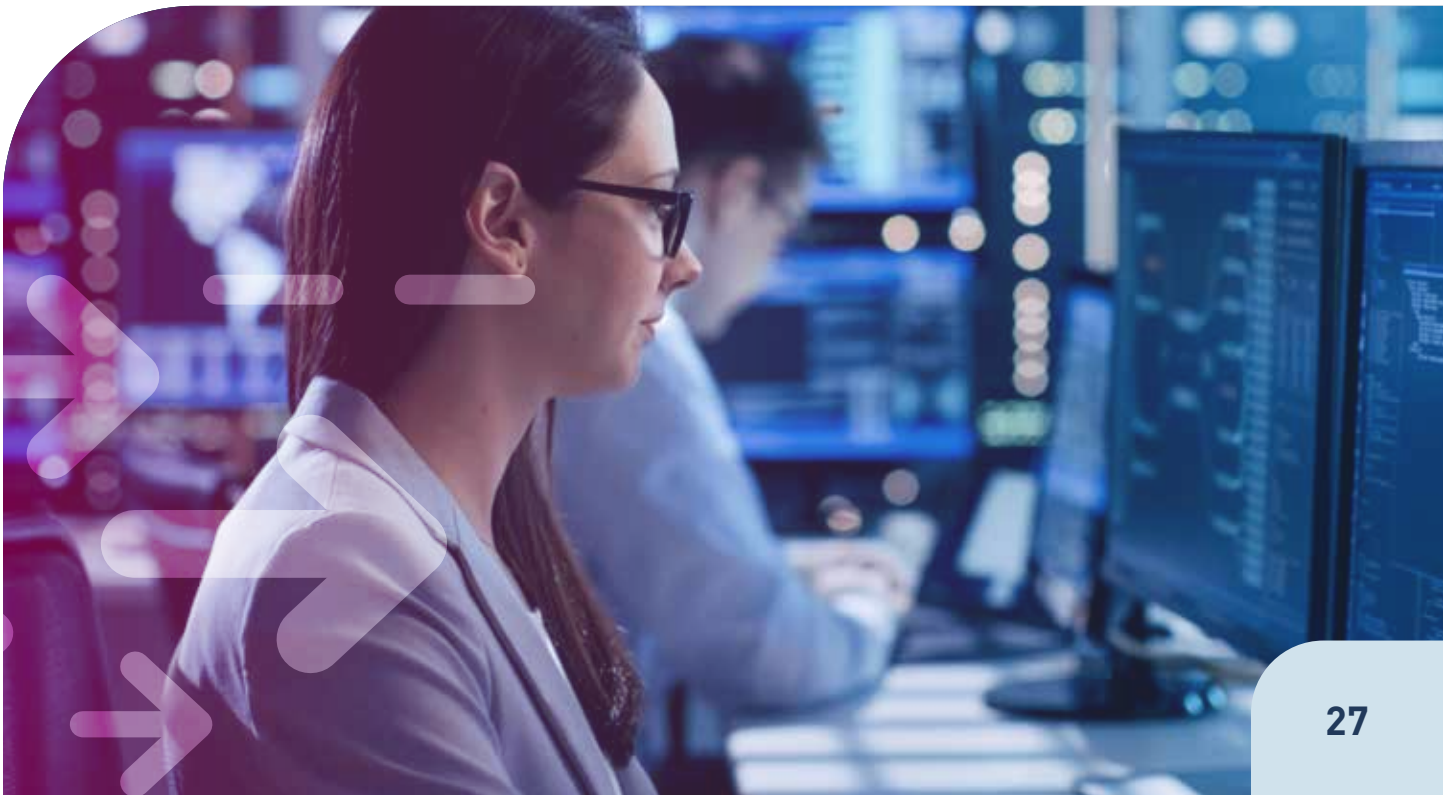
2.4 La cybersécurité : un concept à définir

Le domaine de la cybersécurité étant un secteur d'activité ainsi qu'un champ d'études relativement récent, 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 la Politique gouvernementale de cybersécurité, le Secrétariat du Conseil du trésor mentionne que la cybersécurité correspond à la « [c]apacité, 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 énonce dans la 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 gouvernementale et universitaire provenant d'une variété de pays, a permis de mettre au point une définition qui combine les composantes centrales des définitions recensées. Celle 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 un cyberenvironnement et à ses utilisateurs. (Schatz *et al.*, 2017, p. 66, notre traduction.)



La définition que Schatz, Bashroush et Wall mettent en avant une vision holistique de ce que constitue la cybersécurité; c'est donc celle-ci qui a été retenue pour orienter les analyses dans le présent rapport. L'Institut énonce donc qu'en matière de formation minière, le concept de « cybersécurité » doit être interprété au sens large **à titre d'un ensemble d'approches et d'actions dont l'objet est de développer 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**.

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

Pour les organisations, l'augmentation de la cyberhygiène par l'entremise de l'amélioration des compétences en cybersécurité de la main-d'œuvre constitue une manière efficace 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 et Léger, 2020, p. 16). Ce constat est d'autant plus vrai dans 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 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 de prendre le tournant de l'Internet des objets (Inmarsat, 2020). De plus, lorsque les entreprises se prononcent à propos de ce qu'elles conçoivent comme 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, *Le cadre de référence des compétences à l'ère du numérique dans le secteur minier* a permis d'établir une liste de 23 compétences numériques nécessaires à maîtriser dans les mines à l'ère numérique pour être « numériquement compétent » (Institut national des mines *et al.*, 2020). Regroupées en six familles, ces compétences sont présentées à la **figure 2.**

Figure 2 **Les six familles de compétences numériques selon *Le 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 « Protéger » s'articule en quatre compétences distinctes, qui sont développées dans le **tableau 4**. Dans le cadre de ce rapport, trois des quatre compétences constitutives de cette famille seront considérées comme faisant partie intégrante des compétences en cybersécurité que doit posséder le personnel du secteur minier. Ces trois compétences sont :

1. Utiliser adéquatement et en toute sécurité les équipements numériques;
2. Protéger les données personnelles et corporatives;
3. Gérer les risques.

Bien que la compétence « Adopter des comportements virtuels appropriés » occupe également une place importante dans la protection numérique du secteur minier, l'Institut considère qu'elle ne joue pas un rôle direct dans la prévention des cyberrisques auxquels fait face l'industrie minière. Cette compétence n'est donc pas considérée dans le cadre de ce rapport.

Tableau 4 **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

3. RÉSULTATS DE LA COLLECTE DE DONNÉES

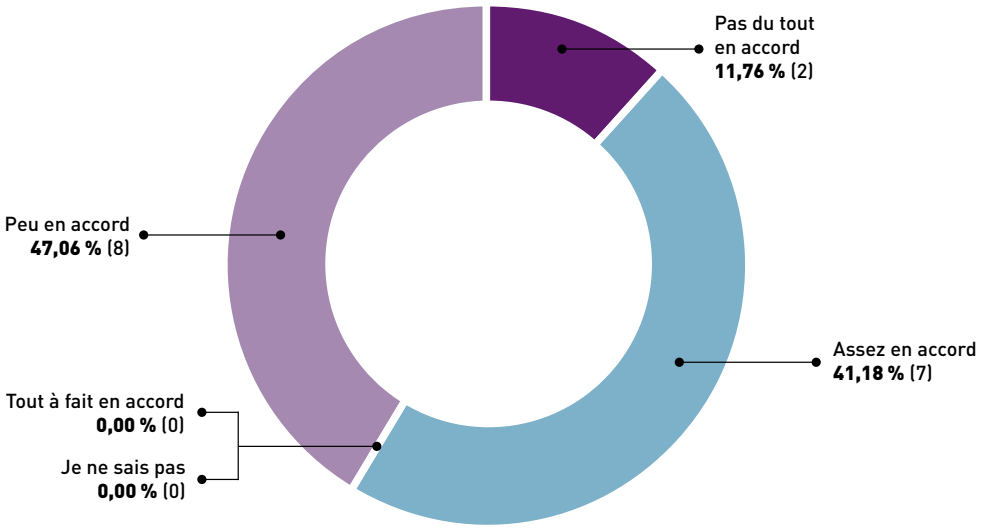
Rappelons que l'objectif de ce projet est de répondre à deux grandes questions liées à la formation minière offerte dans les centres de formation professionnelle et les cégeps du Québec. D'abord, il s'agit de déterminer la place qu'occupe la cybersécurité dans la formation minière québécoise. En d'autres mots, il faut vérifier si les personnes apprenantes qui se destinent à travailler dans le secteur minier sont sensibilisées à la cybersécurité. Ensuite, il faut découvrir la perception des établissements d'enseignement du Québec qui offrent de la formation minière à l'égard de la cybersécurité.

3.1 La sensibilisation aux compétences 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 compétences 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 la compétence « Utiliser adéquatement et en toute sécurité les équipements numériques ». La **figure 3** 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.

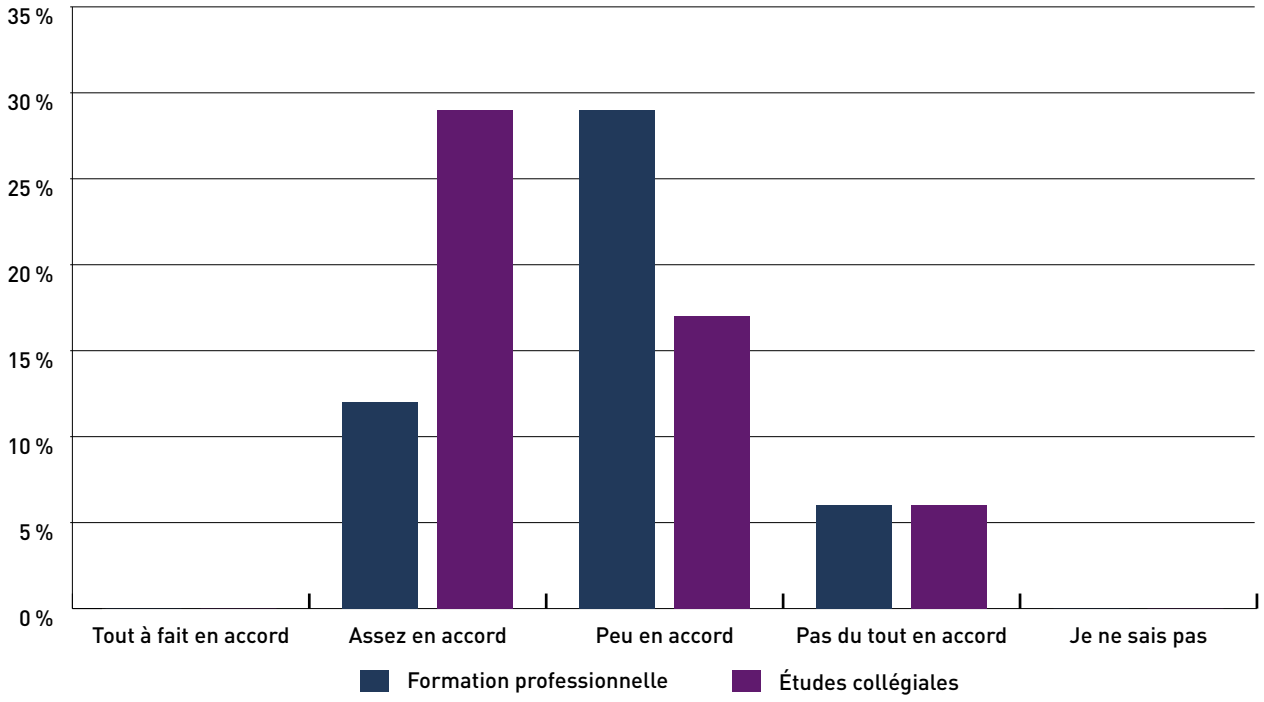
Figure 3 **Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques**



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). »

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 4**, les personnes répondantes émanant des programmes d'études collégiales sont prédominantes parmi les répondantes et les répondants qui considèrent être « Assez en accord » avec l'énoncé selon laquelle 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 la compétence « 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 étudiantes et leurs étudiants sont sensibilisés à cette compétence (25 % des personnes répondantes de cet ordre d'enseignement signalent être « Assez en accord »).

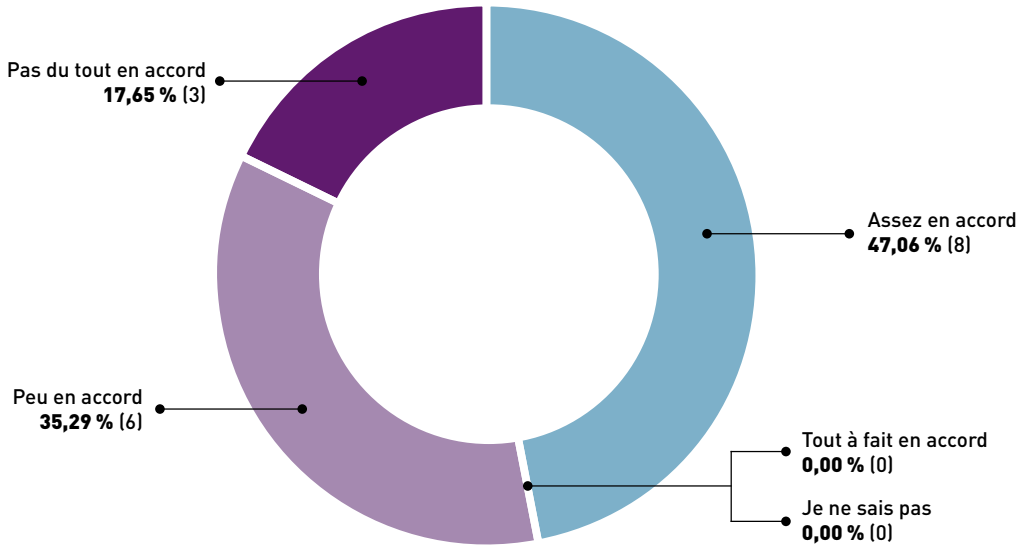
Figure 4 **Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à l'utilisation sécuritaire et préventive des équipements numériques**



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 la compétence « Protéger les données personnelles et corporatives » est présente dans les six programmes de formation et d'études analysés dans ce rapport. La **figure 5** 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.

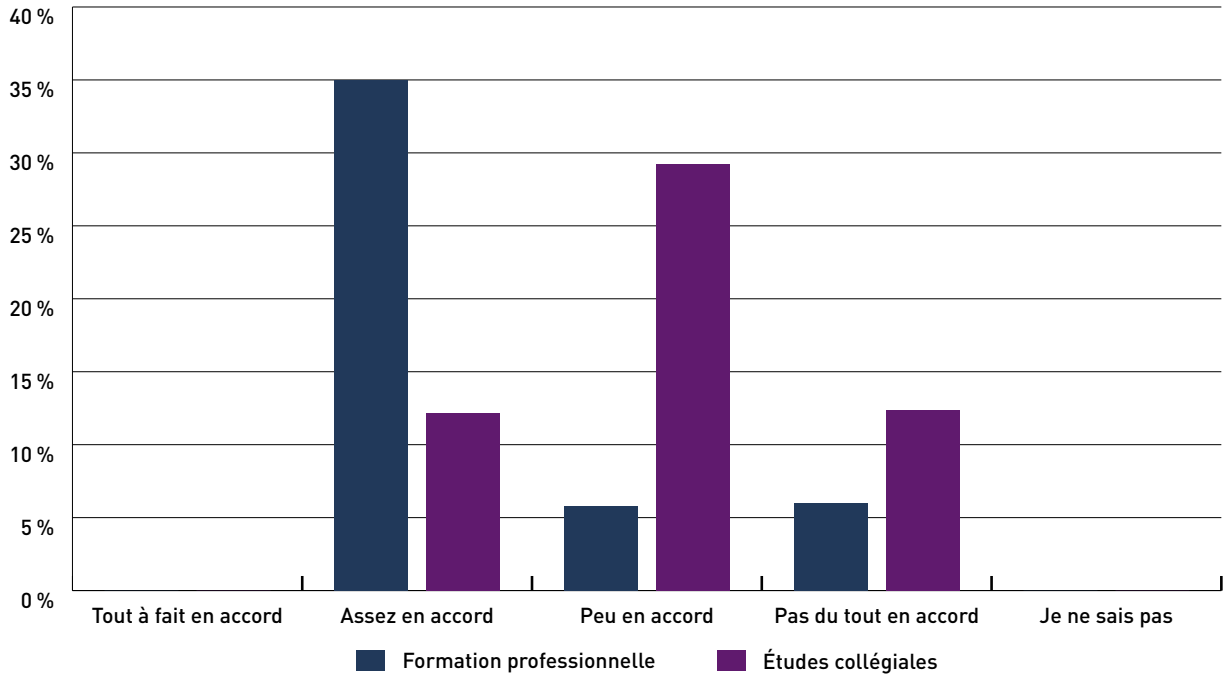
Figure 5 Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations personnelles ou de l'entreprise



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 la compétence 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 renseignements qu'on soit en formation professionnelle ou en formation collégiale. Comme l'indique la **figure 6**, les personnes répondantes provenant des centres de formation professionnelle sont majoritaires parmi les répondantes et les répondants considérant être « Assez en accord » avec l'énoncé selon lequel 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 6** permet de constater que la sensibilisation des personnes apprenantes en formation professionnelle à la compétence « Protéger les données personnelles et corporatives » est effectuée dans la majorité de la formation minière (75 % des personnes répondantes de cet ordre d'enseignement indiquent être « Assez en accord »). La réalité est tout autre dans la formation collégiale, où seulement une faible proportion des personnes répondantes indiquent que leurs personnes apprenantes sont sensibilisés aux notions liées à cette compétence (25 % des personnes répondantes de cet ordre d'enseignement spécifient être « Assez en accord »).

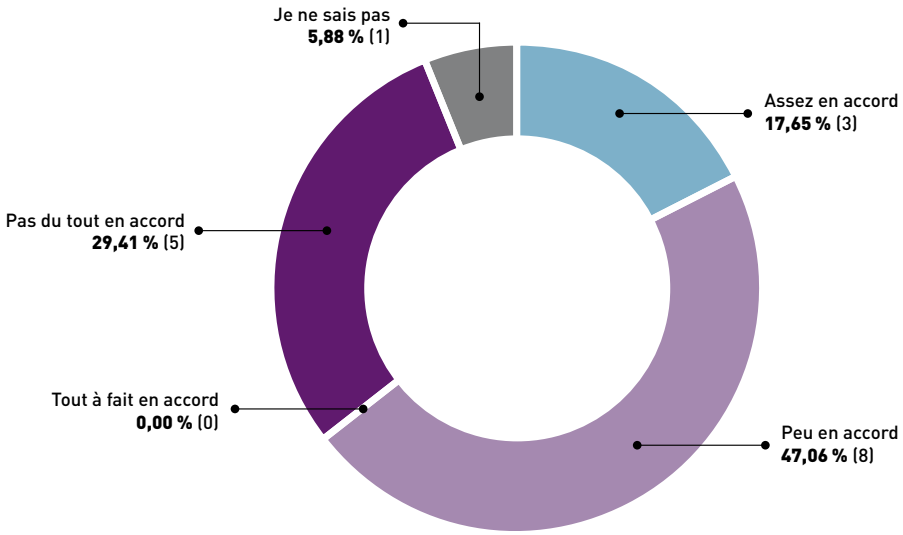
Figure 6 **Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à l'importance d'appliquer les lois et les politiques relatives à la protection des informations personnelles ou de l'entreprise**



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 personnels ou de l'entreprise. »

Par la suite, l'enquête établit dans quelle mesure la sensibilisation à la compétence « Gérer les risques » se retrouve dans les programmes de formation analysés. La **figure 7** 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 %.

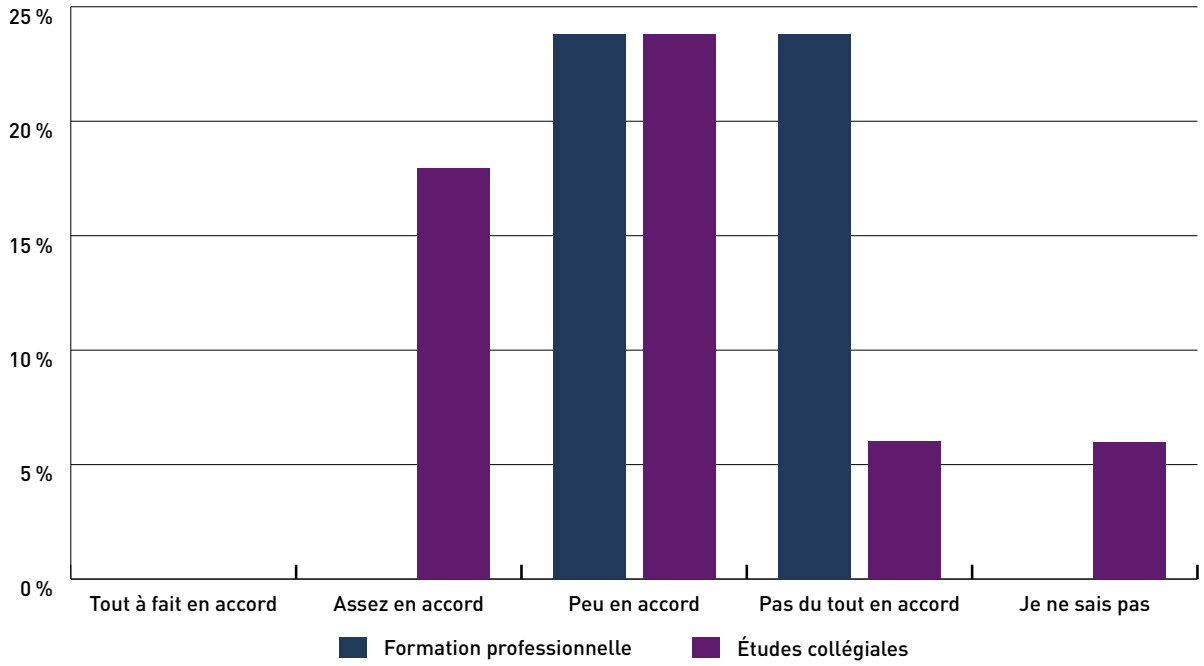
Figure 7 **Niveau d'accord avec le fait que les personnes apprenantes sont sensibilisées à la gestion des risques numériques notamment par l'identification des événements pouvant avoir un impact sur le travail**



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 8** 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 la compétence « 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 la compétence « 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 ».

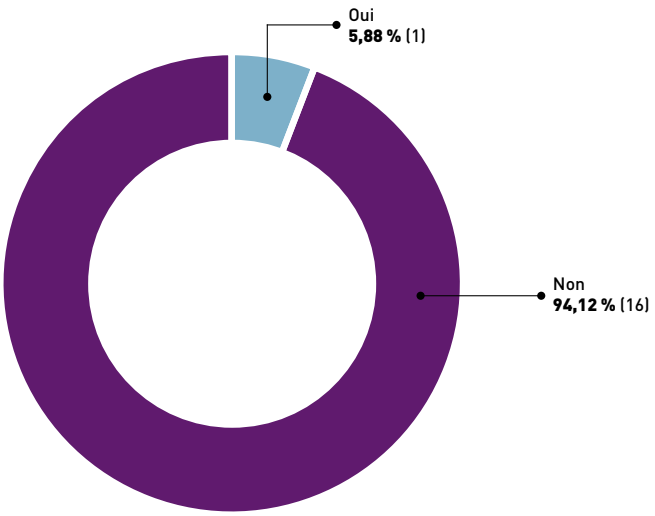
Figure 8 **Niveau d'accord, par ordre d'enseignement, avec le fait que les personnes apprenantes sont sensibilisées à la gestion des risques numériques notamment par l'identification des événements pouvant avoir un impact sur le travail**



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 compétences numériques retenues, d'autres notions relatives à la cybersécurité sont mises en avant dans les six programmes de formation et d'études analysés. La **figure 9** permet de constater que seulement une personne répondante a mentionné que de telles notions sont présentes dans le 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 à la **figure 9** provient de l'ordre d'enseignement collégial.

Figure 9 **Instauration d'autres activités ayant pour objet la sensibilisation à toute notion relative à la cybersécurité**



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

L'examen des résultats précédents permet de dégager une vision globale de la sensibilisation aux compétences en cybersécurité des personnes apprenantes inscrites dans les six programmes de formation et d'études analysés à l'intérieur de ce rapport. Il apparaît que la compétence « Protéger les données personnelles et corporatives » est celle à laquelle les personnes apprenantes sont la plus sensibilisée, suivi de la compétence « Utiliser adéquatement et en toute sécurité les équipements numériques » et, enfin, de la compétence « Gérer les risques ». Il est également intéressant de noter qu'en ce qui concerne chacune de ces compétences, 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 **figures 3**, **5** et **7**. Cela semble signifier qu'aucune personne répondante ne considère que la sensibilisation à l'égard des trois compétences fondamentales en cybersécurité dans le secteur minier ne soit réalisée de manière optimale dans le cadre du programme de formation ou d'études actuellement en vigueur.

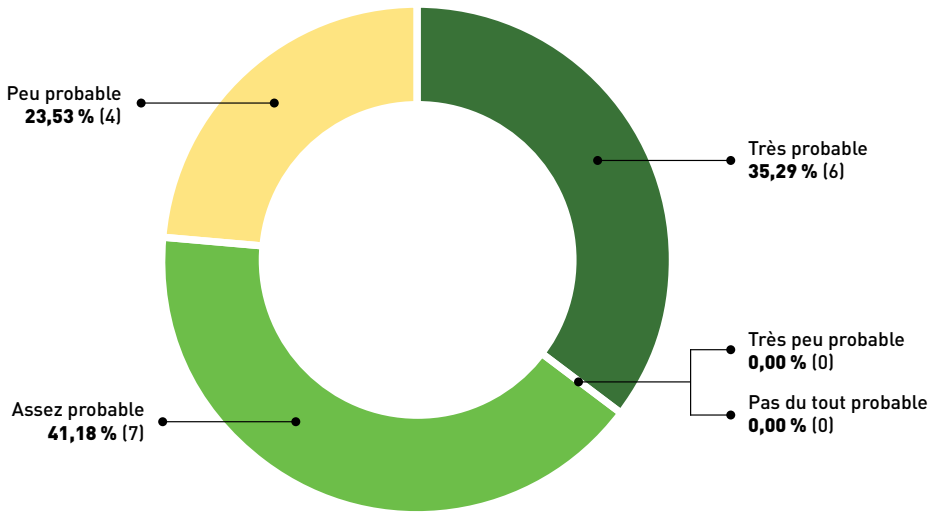
L'examen des résultats de l'enquête offre également l'occasion de faire une analyse par ordre d'enseignement des données collectées. L'étude des **figures 4**, **6** et **8** révèle que la sensibilisation à la cybersécurité pour deux des trois compétences en cybersécurité analysées dans le cadre de ce rapport est prédominante dans les programmes d'études collégiales. De plus, la **figure 9** permet de constater que le seul programme mettant en avant l'apprentissage de notions de cybersécurité complémentaires aux trois compétences de base est un programme d'études collégiales. L'analyse des éléments précédents semble donc indiquer que les trois programmes de formation collégiale analysés sensibilisent davantage leurs étudiantes et leurs étudiants aux compétences en cybersécurité de la famille de compétences « Protéger » 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 à la compétence « Protéger les données personnelles et corporatives » que les programmes d'études collégiales.

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

Dans le cadre de ce rapport, l'Institut a également cherché à déterminer la perception des établissements d'enseignement sondés à l'importance qu'ils accordent à la cybersécurité et à l'apprentissage des compétences liées à celle-ci.

Tout d'abord, le questionnaire a permis d'évaluer dans quelle mesure les personnes répondantes estiment probable qu'au moins une activité pédagogique liée à la cybersécurité soit instaurée dans leur programme de formation ou d'études au cours des deux prochaines années. La **figure 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.

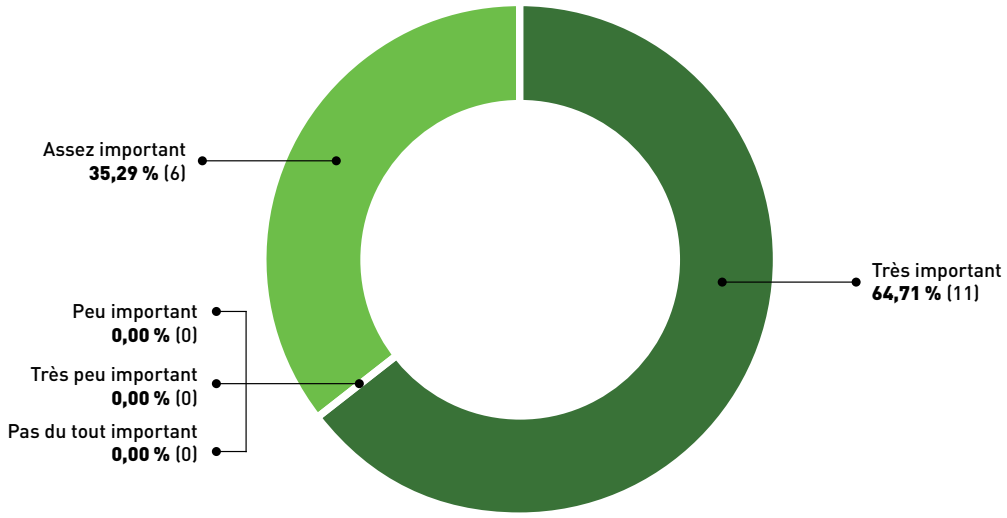
Figure 10 **Probabilité que soient instaurées une ou plusieurs activités pédagogiques visant à sensibiliser les personnes apprenantes à la cybersécurité au cours des deux prochaines années**



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 à la **figure 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 fait que le secteur minier doive tenir compte de la cybersécurité dans ses activités.

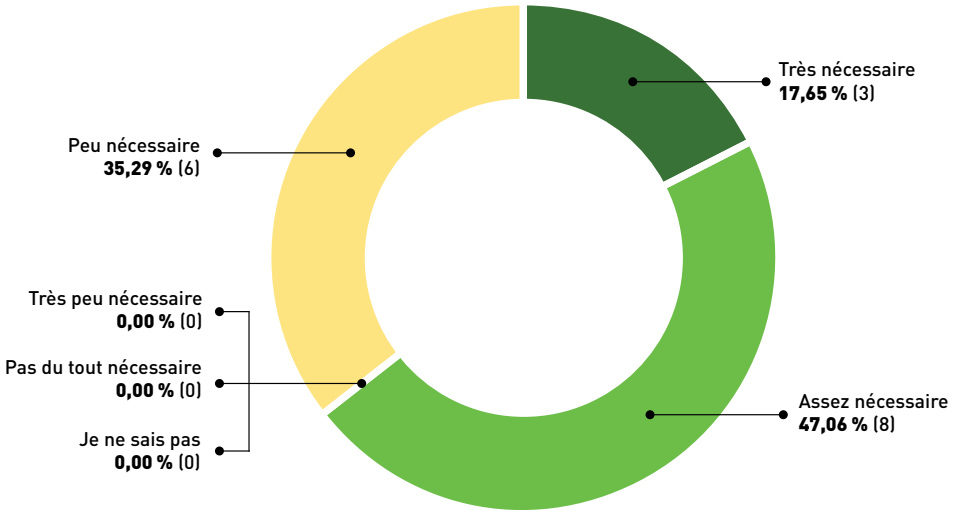
Figure 11 **Perception du niveau d'importance que le secteur minier doit accorder à la cybersécurité dans ses activités**



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. La **figure 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 largement 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.

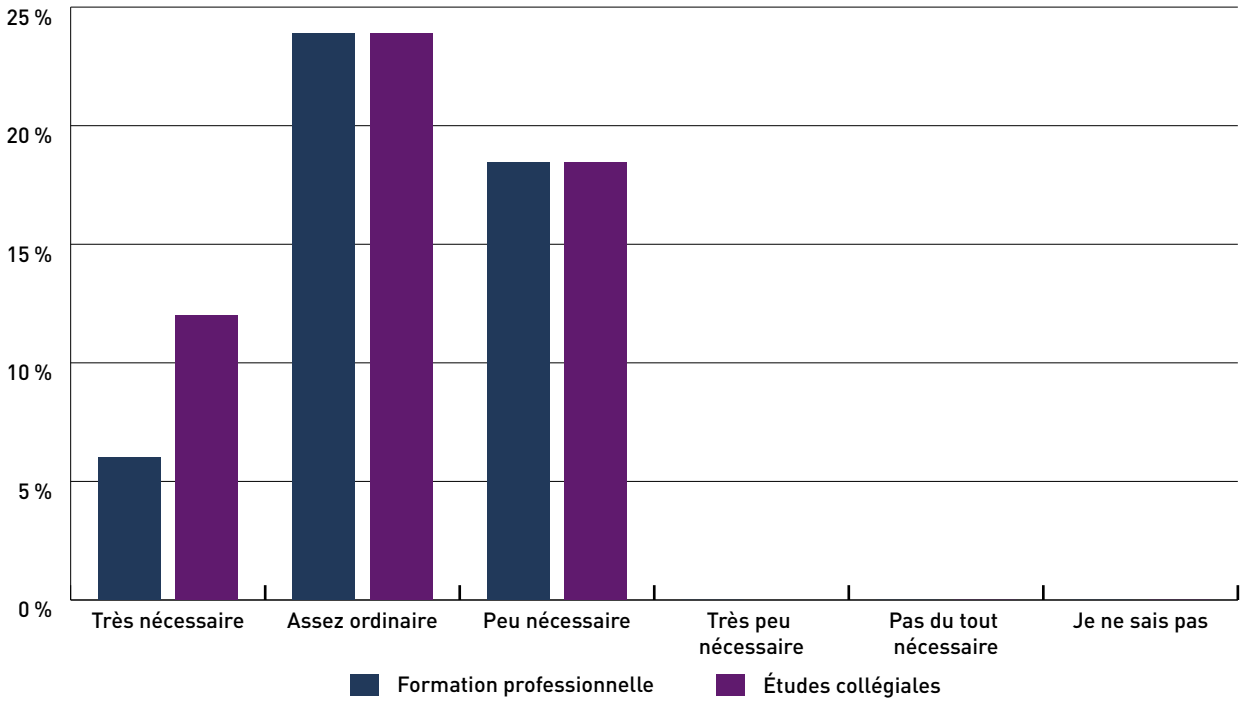
Figure 12 **Perception de la nécessité pour les personnes apprenantes de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier**



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 ? »

La **figure 13** 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.

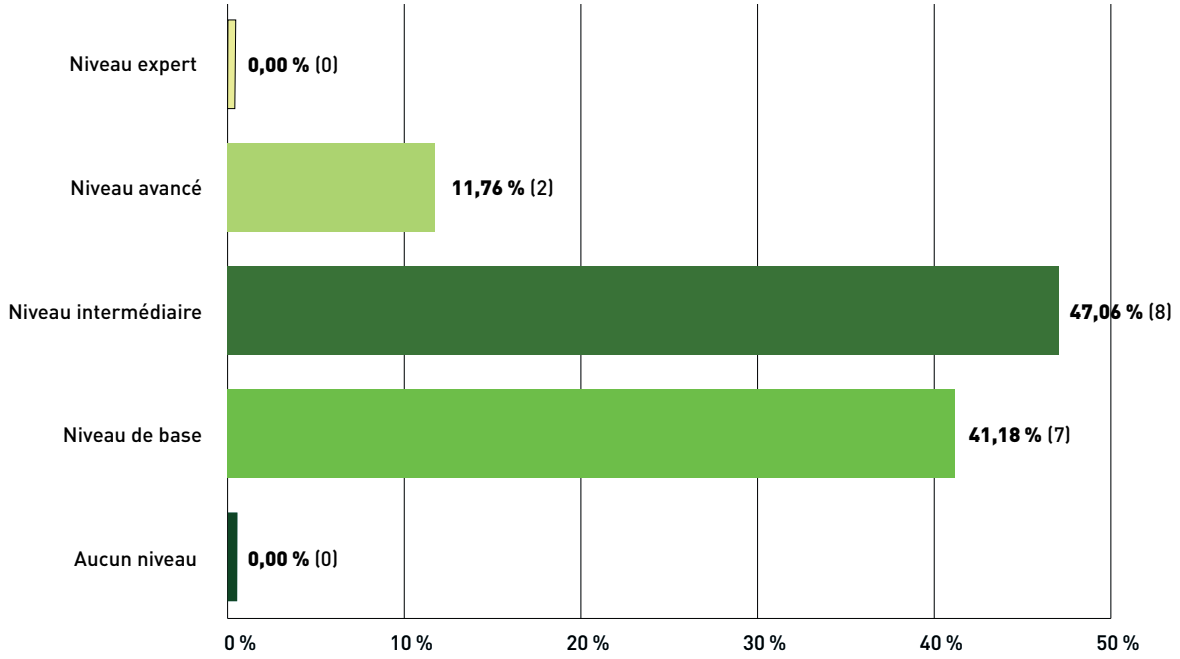
Figure 13 **Perception, par ordre d'enseignement, de la nécessité pour les personnes apprenantes de développer des compétences en cybersécurité pour occuper des postes dans le secteur minier**



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 le niveau de compétence en cybersécurité que devraient détenir les personnes apprenantes inscrites aux programmes analysés. La **figure 14** 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.

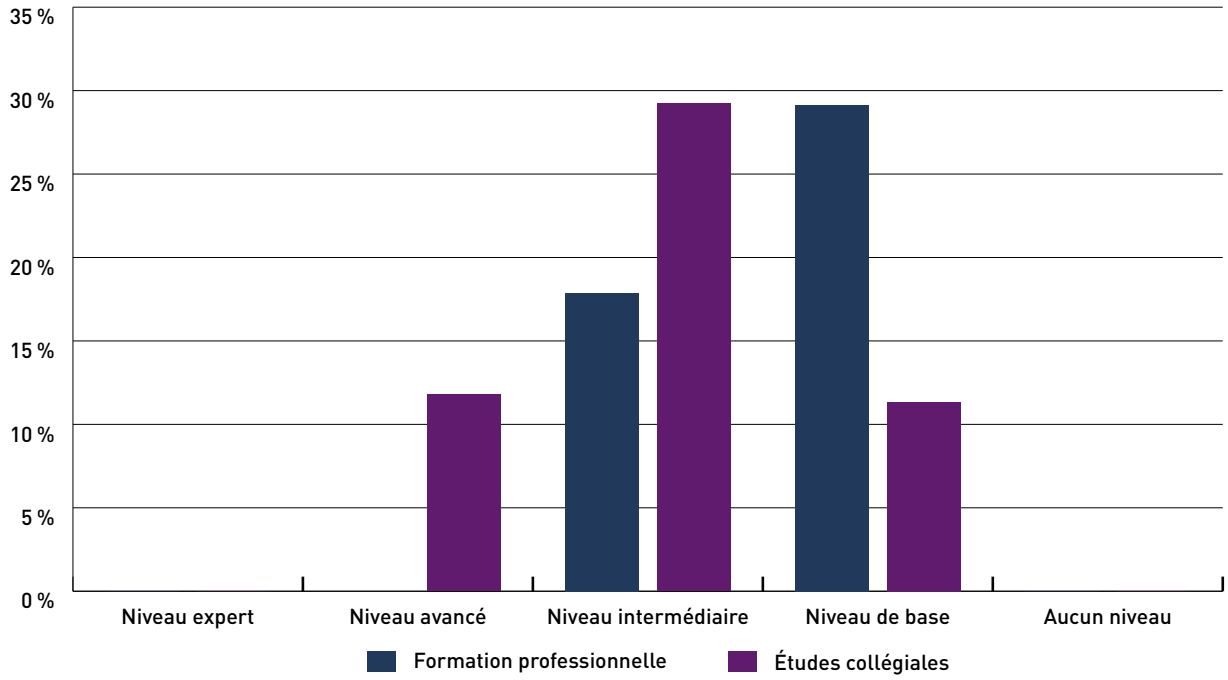
Figure 14 **Perception du niveau de compétence en cybersécurité que doivent posséder les personnes apprenantes pour occuper des postes dans le secteur minier**



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

Les données présentées à la **figure 14** peuvent également être analysées en fonction de l'ordre d'enseignement. Cette approche offre l'occasion 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 que doivent posséder les personnes apprenantes pour occuper des postes dans le secteur minier. La **figure 15** expose que la majorité des personnes répondantes de la formation professionnelle évaluent que les étudiantes et les étudiants 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 largement 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 collégial jugent que les personnes apprenantes doivent posséder un « niveau avancé » de compétence en cybersécurité pour occuper des postes dans le domaine des mines.

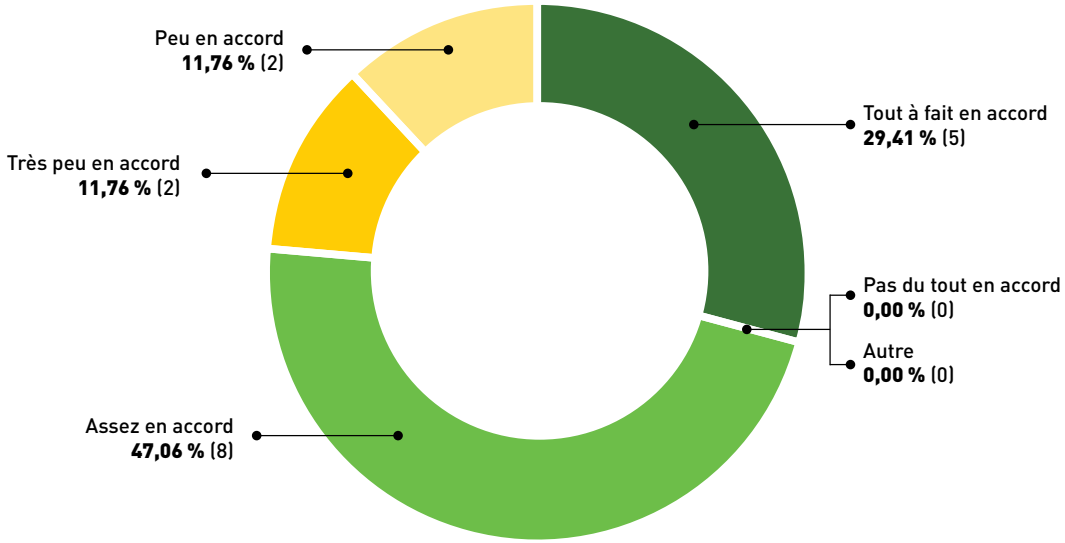
Figure 15 **Perception, par ordre d'enseignement, du niveau de compétence en cybersécurité que doivent posséder les personnes apprenantes pour occuper des postes dans le secteur minier**



Question : « Selon vous, quel niveau de compétence en cybersécurité devraient 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'idée d'inclure l'acquisition d'une compétence liée à la cybersécurité dans la prochaine mise à jour du devis ministériel du programme de formation ou d'études. La **figure 16** illustre que les personnes répondantes sont majoritairement 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.

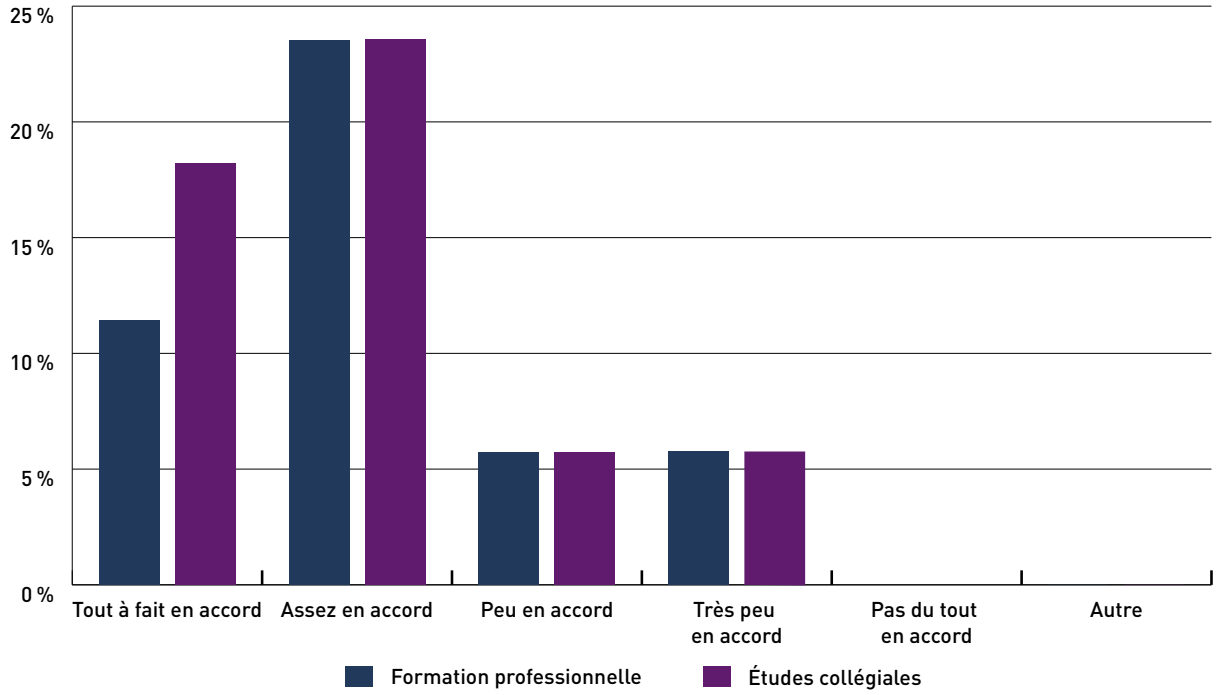
Figure 16 **Niveau d'accord avec l'idée d'inclure l'acquisition d'une compétence liée à la cybersécurité dans le devis ministériel lors de la prochaine mise à jour du programme par le ministère de l'Éducation ou le ministère de l'Enseignement supérieur**



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 liée à la cybersécurité. »

L'examen des données de la **figure 16** en fonction du programme de formation ou d'études au nom duquel les personnes répondantes ont effectué 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 17** montre qu'il existe peu de disparités entre les deux ordres d'enseignement concernant l'idée d'inclure l'acquisition d'une compétence liée 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 % à 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 que doivent posséder les personnes apprenantes qui se destinent 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 17 **Niveau d'accord, par ordre d'enseignement, avec l'idée d'inclure l'acquisition d'une compétence liée à la cybersécurité dans le devis ministériel lors de la prochaine mise à jour du programme par le ministère de l'Éducation ou le ministère de l'Enseignement supérieur**



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 liée 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 qui offrent 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 dans les 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 qu'en formation 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 de compétence en cybersécurité qui doit être acquis, car alors que la majorité des personnes répondantes de la formation professionnelle évaluent qu'un niveau « de base » en cette matière est nécessaire, la majorité des 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 toutefois pas tant la formation professionnelle que collégiale d'être plutôt favorable à l'idée d'inclure l'acquisition d'une compétence liée à la cybersécurité dans les devis ministériels de leurs programmes de formation minière.

L'utilisation de nouvelles technologies dans les programmes d'études en formation professionnelle nécessite l'ajout de compétences notamment en cybersécurité. Dans cette image, un élève du programme de DEP en mécanique d'engins de chantier au Centre de formation professionnelle de la Baie-James effectue ses travaux à l'aide d'un ordinateur. (Photographe : Joël Lavoie)

4. ANALYSE DES RÉSULTATS

Dans le cadre de cette enquête, l'Institut a 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 compétences 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. En effet, que ce soit en ce qui concerne la compétence « Utiliser adéquatement et en toute sécurité les équipements numériques », la compétence « Protéger les données personnelles et corporatives » ou encore la compétence « 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 programmes de formation minière les plus recherchés par l'industrie procurent peu de sensibilisation en dehors de celle destinée à rehausser la maîtrise des trois compétences, 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 compétences 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 recherchés au sein de l'industrie minière. Les données colligées montrent que les établissements d'enseignement qui offrent la formation minière la plus recherchée par le secteur minéral sont conscients de l'importance que revêt la cybersécurité dans cette industrie en 2020. Ils 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 compétences « Utiliser adéquatement et en toute sécurité les équipements numériques », « Protéger les données personnelles et corporatives » et « Gérer les risques » font respectivement l'objet d'une sensibilisation dans une minorité de programmes de formation minière professionnelle et collégiale. Par conséquent, il est possible de constater 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 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 recueillies 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 recherchés 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 compétences 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.

La mise en place d'une cybersécurité efficace constitue désormais une priorité pour les sociétés du secteur minier. Avec le réseau LTE sous terre, le personnel d'Agnico Eagle est bien conscient des enjeux liés à la sécurité des données et des actifs numériques. (Photographe : Mathieu Dupuis)

5. PISTES DE RECHERCHE

En s'appuyant sur les données collectées et analysées, l'Institut estime que plusieurs recherches supplémentaires pourraient être menées en vue 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 l'avenir. En effet, puisque le présent rapport s'est concentré sur les programmes de formation professionnelle et de formation collégiale, 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 dans le monde 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 pour pousser plus loin la réflexion en matière de cybersécurité en formation minière consisterait à analyser la formation relative à la cybersécurité qu'offrent 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.

L'amélioration des compétences en cybersécurité constitue un impératif au secteur minéral à l'ère de la mine intelligente. Chez ArcelorMittal, deux techniciens s'affairent à diagnostiquer un code d'erreur sur un équipement mobile tout en s'assurant des bonnes pratiques en gestion de données. (crédit photo : ArcelorMittal)

CONCLUSION

En conclusion, dans ce rapport, l'Institut a cherché à mieux situer la place que la cybersécurité est appelée à occuper dans les curriculums menant à l'exercice d'un métier ou d'une profession du secteur minier à l'ère du numérique. L'Institut a par la suite voulu analyser la place accordée à la cybersécurité dans la formation minière dispensée dans les établissements d'enseignement du Québec qui offrent de la formation minière ainsi que la perception de ces établissements à l'égard de la cybersécurité.

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 compétences en cybersécurité qui sont 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'effectuent pas de sensibilisation.

La perception des programmes de formation professionnelle et d'études collégiales en formation minière à l'égard de la cybersécurité est également mieux définie grâce à ce rapport. En effet, nous savons désormais que les personnes répondantes des programmes de formation analysés considèrent que les entreprises du secteur minier doivent accorder de l'importance à la cybersécurité dans le cadre de leurs activités et que, par conséquent, le développement de compétences en cybersécurité est nécessaire chez les personnes apprenantes qui désirent 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 la majorité que les personnes apprenantes qui désirent travailler dans le secteur minier doivent posséder des compétences de niveau intermédiaire ou de base en cybersécurité, et que cette perception fait en sorte que la majorité se positionne favorablement par rapport à l'idée d'inclure une compétence en cybersécurité dans les devis ministériels.

Notre compréhension de la cybersécurité en formation minière est rehaussée grâce à ce rapport qui nous a permis de faire progresser non seulement notre connaissance 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 l'avenir de l'éducation au Québec.

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 données 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 qui permettent d'améliorer la protection des données 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 activités pédagogiques de sensibilisation effectuées 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 activités pédagogiques de sensibilisation effectuées 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 activités pédagogiques de sensibilisation effectuées ainsi que leurs objectifs.

*** 11. Avez-vous, dans le cadre du programme d'études actuellement en vigueur, instauré toute autre activité ayant pour objet 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 activités de sensibilisation effectuées ainsi que leurs objectifs.

*** 13. 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 ?**

- ☐ 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 devraient 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 liée 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**

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

RÉFÉRENCES

Austmine (2018). *Cyber security in mining operations*. http://www.austmine.com.au/Publications/category/publications/cyber-security-in-mining-operations-ebook

Baylon, C. (2014). *Challenges at the Intersection of Cyber Security and Space Security : Country and International Institution Perspectives*, Royal Institute of International Affairs. https://www.chathamhouse.org/2014/12/challenges-intersection-cyber-security-and-space-security-country-and-international

CDW Canada (2020). *Cyber Resilience: An Evolving Perspective*. https://fr.cdw.ca/content/cdwca/en/solutions/cybersecurity/security-study.html

CISCO (2020). *What Is Cybersecurity?* CISCO. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Comité sectoriel de main-d'oeuvre de l'industrie des mines (2020). *Estimation des besoins de main-d'oeuvre du secteur minier au Québec : 2019-2023 avec tendances 2028*. https://www.explorelesmines.com/images/pdf/Section_corporative/Publications/Etudes_sectorielles/EBMO_final.pdf

Deloitte (2018). *An integrated approach to combat cyber risk: Securing industrial operations in mining*. https://www2.deloitte.com/global/en/pages/energy-and-resources/articles/approach-to-combat-cyber-risk-mining.html

Ernst & Young et Associés (2018). *Does cyber risk only become a priority once you've been attacked?: Mining and metals*. https://www.ey.com/Publication/vwLUAssets/ey-cyber-in-mining-report/$File/EY-cyber-in-mining-report.pdf

Forum économique mondial (2017). *Digital Transformation Initiative Mining and Metals Industry*. http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/wef-dti-mining-and-metals-white-paper.pdf

Inmarsat (2020). *The Rise of IoT in Mining*. https://research.inmarsat.com/2020/download-report/

Institut de la statistique du Québec (2019). *Mines en chiffres—L'investissement minier au Québec en 2018*. https://bdso.gouv.qc.ca/docs-ken/multimedia/PB01633FR_mine2018H00F00.pdf

Institut de la statistique du Québec (2020). *Mines en chiffres—La production minérale au Québec en 2018*. https://bdso.gouv.qc.ca/docs-ken/multimedia/PB01633FR_mine2018H00F01.pdf

Institut national des mines (2018a). *Les tendances générales en formation minière en 2018*. https://inmq.gouv.qc.ca/medias/files/Publications/Rapports_de_recherche/INMQ_Tendances_generales_formation_miniere_11_janv_28juin2018.pdf

Institut national des mines (2018b). *Transformation numérique et compétences du 21e siècle pour la prospérité du Québec—Exemple de l'industrie minière*. https://inmq.gouv.qc.ca/medias/files/Publications/Rapports_de_recherche/INMQ_Transformation_numerique_complet.pdf

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*. https://inmq.gouv.qc.ca/medias/files/Publications/Rapports_de_recherche/Cadre_references_metiers/INMQ_Cadre_reference_competence_ere_numerique.pdf

Jenish, D. (2018). *Miners band together to fight cyber-criminals: How the industry is fighting back and beefing up cyber-security*, Canadian Mining Journal. http://www.canadianminingjournal.com/features/miners-band-together-to-fight-cyber-criminals/

Kohler, D. et J.-D. Weisz (2016) Industrie 4.0 : comment caractériser cette quatrième révolution industrielle et ses enjeux ? *Annales des Mines - Réalités industrielles*, novembre 2016(4), 51-56.

Li, L., W. He, L. Xu, I. Ash, M. Anwar et X. Yuan (2019). "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, 45, 13-24.

Ma, Q., M. Schmidt et M. Pearson (2009). "An Integrated Framework for Information Security Management", *Review of Business*, 30(1), 58-69.

Marsh (2018). *Cyber Risk : Threats and Insurance Protection for the Mining Sector*. https://www.marsh.com/uk/insights/research/cyber-risk-threats-and-insurance-protection-for-the-mining-sector.html

Marsh et Microsoft (2019). *2019 Global Cyber Risk Perception Survey*. https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

Ministère de l'Économie et de l'Innovation (2016). « Industrie 4.0 : les défis de la quatrième révolution industrielle », *Bulletin Espace Conseils PME*. 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 », *Bulletin Espace Conseils PME*. 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 », dans *Les sous-secteurs/Logiciel*. 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*. http://www.education.gouv.qc.ca/fileadmin/site_web/documents/ministere/Cadre-reference-competence-num.pdf

NOVIPRO et Léger (2020). *Portrait des TI dans les moyennes et grandes entreprises canadiennes*. https://hub.novipro.com/fr/portrait-des-ti-2020

PwC (2020a). *23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty*. https://www.pwc.com/gx/en/ceo-survey/2020/reports/pwc-23rd-global-ceo-survey.pdf

PwC (2020b). *Mines 2020—Minières canadiennes : ingéniosité et résilience*. https://www.pwc.com/ca/fr/industries/mining/mine-2020.html

RSA Security (2016). *Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise*. https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf

Schatz, D., R. Bashroush et J. Wall (2017). "Towards a More Representative Definition of Cyber Security", *Journal of Digital Forensics, Security and Law*, 12(2), 53-74. https://commons.erau.edu/cgi/viewcontent.cgi?article=1476&context=jdfsl

Secrétariat du Conseil du trésor (2020). *Politique gouvernementale de cybersécurité*. https://www.quebec.ca/gouv/politiques-orientations/vitrine-numeriqc/politique-gouvernementale-de-cybersecurite/

Sécurité publique Canada (2018). *Stratégie nationale de cybersécurité : vision du Canada pour la sécurité et la prospérité dans l'ère numérique*. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-fr.pdf

Soomro, Z. A., M. H. Shah et J. Ahmed (2016). "Information security management needs more holistic approach : A literature review", *International Journal of Information Management*, 36, 215-225.

Willis Towers Watson (2017). *From technology to people: The new frontier in mining cyber risk*. https://www.willistowerswatson.com/en/insights/2017/09/mining-risk-review-from-technology-to-people-the-new-frontier-in-mining-cyber-risk

125, rue Self
Val-d'Or (Québec) J9P 3N2

Téléphone : 819 825-4667
info@inmq.gouv.qc.ca
inmq.gouv.qc.ca