UNIVERSITÉ DU QUÉBEC À MONTRÉAL

DÉTERMINANTS DE LA DIVULGATION EN MATIÈRE DE CYBERSÉCURITÉ DES ENTREPRISES

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

MAÎTRISE EN COMPTABILITÉ, CONTRÔLE, AUDIT

PAR

ORIANNE AHOCOU

AVRIL 2026

REMERCIEMENTS

Tout d'abord, je remercie Dieu le tout-puissant de m'avoir aidée dans les moments les plus difficiles à accomplir cette recherche et de m'avoir guidée à travers mes choix dans ce travail.

Selon Beau & al. (2005), « aucun travail ne s'accomplit dans la solitude ». Ainsi, je ne peux m'empêcher d'exprimer mes sincères remerciements à toutes les personnes qui se sont investis d'une manière ou d'une autre de près ou de loin dans la réussite de mon cursus et dans la rédaction de mon mémoire de fin de parcours.

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.

Je voudrais, dans un premier temps, remercier, ma directrice de recherche, madame Camélia Radu, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je voudrais exprimer ma profonde gratitude à l'École des sciences de la gestion de l'Université du Québec à Montréal (ESG-UQAM) pour la qualité de l'enseignement reçu, pour le soutien académique rigoureux et pour les ressources mises à notre disposition. Je tiens également à remercier l'institution pour le soutien financier qui m'a été offert par le biais des bourses d'excellence, qui ont représenté une précieuse source de motivation.

Je tiens à témoigner toute ma reconnaissance :

- Aux membres du jury, qui, malgré leur emploi du temps chargé, m'ont fait l'honneur d'examiner ce modeste travail ;

- À mes professeurs, mesdames Hanen Khemakhem, Audrey de Rancourt-Raymond Messieurs Richard Fontaine, Yakoma Koudema pour leur disponibilité, remarques et précieux conseils qui ont contribué à l'enrichissement de mes connaissances et à la réussite de ce travail.

- À mes camarades de promotion, pour le capital relationnel créé, pour l'amour et la sincérité qui ont été pour moi une excellente source de réconfort et d'inspiration.

Enfin, toute ma gratitude va à l’endroit de mes parents et de ma famille, pour leur soutien constant et leurs encouragements.

DÉDICACE

À

- Mes chers parents, Alexandre et Odette
- Mon cher grand frère Mike
- Mon cher oncle Daniel et sa femme Eugenia
- Mes cousines Elouan et Gifty

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES

ACVM	**:**	Autorité canadienne en Valeurs mobilières
AICPA	**:**	American Institute of Certified Public Accountants
CA	**:**	Conseil d'administration
CPA	**:**	Comptable Professionnel Agréé
DivCyb	**:**	Divulgation de cybersécurité
DiverCA	**:**	Diversité de genre du conseil
EPE	**:**	Émetteurs privés étrangers
FD	**:**	Fair disclosure
IC	**:**	Intervalle de confiance
IndCA	**:**	Indépendance du conseil
Indus	**:**	Industrie ou secteur d'activité
MENA	**:**	Middle East and Northern Africa
OICV	**:**	Directeur Commercial
OSL	**:**	Ordinary Least Squares
RBV	**:**	Resource-Based View

Rent	**:**	Rentabilité
SEC	**:**	Securities and Exchange Commission
S&P/TSX60	**:**	Bourse de Toronto
SPSS	**:**	Statistical Package for the Social Sciences
TailCA	**:**	Taille du conseil
TailEnt	**:**	Taille de l'entreprise
VRIN	**:**	Valuable, Rare, Inimitable et Non substituable

RÉSUMÉ

Ce mémoire examine les déterminants de la divulgation en matière de cybersécurité effectuée par les entreprises. Actuellement, avec la recrudescence des cyberrisques, la transparence dans le partage d'informations sur la cybersécurité devient une stratégie adoptée par les entreprises pour combler les besoins en informations des parties prenantes à cet effet. En s'appuyant sur la théorie des ressources et du signal, cette étude cherche à identifier les facteurs, plus précisément les caractéristiques du conseil d'administration (taille, indépendance, diversité de genre, expertise en technologies de l'information) susceptibles d'influencer le niveau de divulgation de cybersécurité. Elle est réalisée sur un échantillon de 60 grandes entreprises cotées à la bourse de Toronto, sur une période de 3 ans allant de 2021 à 2023. La méthodologie adoptée repose une approche mixte combinant une analyse de contenu automatisé via Nvivo afin de mesurer la divulgation de cybersécurité dans les rapports et des tests de régression logistiques et linéaires pour tester les hypothèses de recherche. Les résultats démontrent que l'indépendance et l'expertise en technologies de l'information des membres du conseil impactent positivement et significativement le niveau de divulgation, tandis que la taille n'exerce aucun effet significatif sur celle-ci. Par ailleurs, les résultats indiquent que la diversité du conseil est un déterminant du choix de publier (ou pas) de l'information concernant la cybersécurité, tandis qu'elle n'a pas d'influence sur le volume de l'information publiée. Ce mémoire contribue au développement de la littérature sur la gouvernance et la transparence en cybersécurité dans le contexte canadien.

Mots-clés : Divulgation de cybersécurité, caractéristiques du conseil d'administration, théorie du signal, théorie des ressources, cybersécurité, déterminants

ABSTRACT

This thesis focuses on the determinants of cybersecurity disclosure by companies. Currently, with the rise in cyber risks, transparency in sharing cybersecurity information is becoming a strategy adopted by companies to meet the information needs of stakeholders. Drawing on resource-signal theories, this study seeks to identify the factors, specifically board characteristics (size, independence, gender diversity, IT expertise), that may influence the level of cybersecurity disclosure. It is conducted on a sample of 60 large companies listed on the Toronto Stock Exchange over a three-year period from 2021 to 2023. The methodology employed is a mixed-methods approach combining automated content analysis using Nvivo to measure cybersecurity disclosure in reports and logistic and linear regression tests to test the research hypotheses. The results demonstrate that the independence and information technology expertise of board members positively and significantly impact the level of disclosure, while board size has no significant effect. Furthermore, the results indicate that board diversity is a determinant of the decision to publish (or not) cybersecurity information, but it does not influence the volume of information published. This thesis contributes to the development of the literature on governance and transparency in cybersecurity within the Canadian context.

Keywords: Cybersecurity disclosure, board characteristics, signaling theory, resource-based view, cybersecurity, determinants

INTRODUCTION

Notre monde, loin d'être statique, est dynamique et porte en lui les facteurs internes qui sont continuellement responsables des transformations structurelles qui façonnent son image au fil du temps. Aujourd'hui, sans nul doute, nous vivons pleinement dans l'ère de la révolution numérique, qui va certainement s'amplifier avec le développement de l'intelligence artificielle. Cette évolution si remarquable de notre monde se déroule certes avec beaucoup d'aspects positifs et bénéfiques au genre humain, mais il y a aussi et malheureusement des déviations caractérisées et mal intentionnées qui impactent négativement l'humain et le climat des affaires. C'est le cas de la cybercriminalité, par exemple, qui impacte tous les secteurs d'activités et qui empoisonne l'environnement économique à tous ses échelons.

La prépondérance du phénomène des cyberattaques en vogue, a fait réagir l'ex-ministre canadien de la Défense, Mme Anita Anand, qui soutient que « les menaces évoluent au même rythme que les progrès fulgurants qui ont été réalisés sur le plan de la technologie » [1]. Le Centre canadien pour la cybersécurité définit la cybermenace comme « une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient, ou à perturber le monde numérique en général » [2]. Habituellement, ces cyberattaques prennent principalement la forme de violation de données, ou de rançongiciels, mais peuvent aussi se décliner sous la forme de différentes autres intrusions. Cela dit, les cybercriminels, dont la principale motivation est pécuniaire, prennent en otage les organisations à travers le contrôle de leur système d'information et en volant des données confidentielles en vue de perturber ou de paralyser totalement les activités de ces dernières. Le retour à la normale est assujetti au paiement de fortes sommes d'argent versées aux cybercriminels par les organisations victimes. À cet effet, en 2023, 85% des organisations canadiennes ont été victimes de cyberattaques. Nous avons, par exemple, la chaîne de librairies canadiennes Indigo, qui a été victime d'une attaque de rançongiciel majeure, ayant perturbé ses systèmes de paiement pendant plusieurs jours et lui ayant coûté environ 50 millions de dollars. Nous avons également les

[1] https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024, consulté le2025/11/24

[2] https://www.cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces , consulté le 2025/11/24

cas populaires, Desjardins et Equifax, survenus respectivement en 2019 et 2017, occasionnant en termes de coûts 108 millions de dollars pour le premier et 425 millions de dollars pour le second.

Les conséquences d'une cyberattaque sont très dommageables et de diverses natures pour les entreprises victimes. De pertes financières en passant par l'atteinte à leurs réputations, ces entreprises doivent aussi faire face à la dégradation de la confiance des parties prenantes. De ce fait, le Ponemon-Institute, dans son rapport intitulé " 2017 Cost of Data Breach Study: United States " (2017), a identifié deux types de coûts comme conséquences liées à la violation des données. Il s'agit :

- des coûts directs que sont les coûts immédiats liés à la gestion de la violation, comme les enquêtes, les services de notification, les mesures de sécurité supplémentaires et les amendes potentielles;

- des coûts indirects incluant la perte de clients, la baisse de la réputation et la diminution de la confiance des parties prenantes.

Face à sa recrudescence, à ses risques inhérents croissants ainsi qu'à ses conséquences pernicieuses, la cybersécurité est aujourd'hui au centre de toutes les attentions autant pour l'entreprise et ses parties prenantes que pour les régulateurs.

Masoud et Al-Utaibi (2022), ressortant l'importance de la cybersécurité, citent L'American Institute of Certified Public Accountants (AICPA) (2018, p.1) en ces termes, « la cybersécurité est l'une des principales préoccupations des dirigeants et des conseils d'administration de presque toutes les entreprises du monde - grandes et petites, publiques et privées ». Les parties prenantes (investisseurs, clients, fournisseurs, etc.) se sentent très concernées par la sécurité et la protection de leurs données. Ils ont un besoin continuel de s'informer auprès des entreprises sur leur cybersécurité.

La divulgation étant une manière pour les entreprises de répondre aux besoins en informations de leurs parties prenantes, elles adoptent par conséquent une stratégie de divulgation en matière de cybersécurité. Suite à l'importance significative de la cybersécurité aujourd'hui, les régulateurs se

sont eux aussi penchés sur la question. Ainsi, la Securities and Exchange Commission (SEC) des États-Unis met à jour les directives publiées en 2011 dans le but de s'assurer que les entreprises fournissent des informations pertinentes aux investisseurs concernant les menaces et incidents de cybersécurité. Ces exigences obligent les entreprises cotées en bourse à divulguer à la fois les incidents importants de cybersécurité qu'elles connaissent, ainsi que des informations matérielles concernant leur gestion des risques de cybersécurité, leur stratégie et leur gouvernance. Cette initiative a pour objectif de fournir aux investisseurs des informations plus opportunes, cohérentes, comparables, transparentes et utiles à la prise de décision (Gerding, 2023). Ainsi, la divulgation en matière de cybersécurité est devenue une pratique standard que toutes les entreprises ont tendance à adopter et faisant partie de leur stratégie de gestion des risques.

Étant donné que la cybersécurité est un nouveau concept qui prend de l'ampleur, les auteurs également ont commencé à s'y intéresser et à mener des recherches dans ce sens. Plusieurs études ont été menées sur ses tendances, ses pratiques et ses implications. Certaines se sont penchées sur l'influence des caractéristiques du conseil d'administration, notamment la taille (Alodat *et al.*, 2024 ; Mazumder et Hossain, 2023 ; Smaili *et al.*, 2023), l'indépendance (Alodat *et al.*, 2024 ; Héroux et Fortin, 2024 ; Lim *et al.*, 2007 ; Mazumder et Hossain, 2023 ; Shukla et Pandey, 2023), la diversité de genre (Kurnia et Ardianto, 2024 ; Radu et Smaili, 2022), l'efficacité et l'expertise financière (Smaili *et al.*, 2023) et l'expertise technique (Al-Sartawi, 2020 ; Chen *et al.*, 2022 ; Héroux et Fortin, 2024 ; Shukla et Pandey, 2023) sur la divulgation en matière de cybersécurité. D'autres sur les influences des nouvelles directives de la SEC (*2024 Canada Spencer Stuart Board Index Snapshot*, 2024 ; Calderon et Gao, 2022 ; Li *et al.*, 2018 ; Wang *et al.*, 2022).

Cependant, bien que toutes ces études explorent les contours de la divulgation sur la cybersécurité, il est important d'investiguer les facteurs qui déterminent la divulgation volontaire ou obligatoire d'informations en matière de cybersécurité par les entreprises. Mazumder et Hossain (2023) ont examiné les facteurs qui influencent la divulgation volontaire de la cybersécurité dans les banques commerciales cotées en bourse au Bangladesh, mais se sont concentré la composition du conseil d'administration en matière de diversité. Sari et al. (2024) ont réalisé une revue de littérature systématique sur les facteurs déterminants de la divulgation d'information en matière de cybersécurité. Ils concluent que les facteurs déterminants de cette divulgation sont la taille du conseil d'administration, son indépendance, la diversité au sein du conseil d'administration, les

actionnaires institutionnels, les actionnaires étrangers, les cyberincidents antérieurs, la violation par les pairs, l'attention du public, les dépenses en capital, l'actif incorporel, la taille, la croissance et l'endettement de l'entreprise.

Les Autorités canadiennes en valeurs mobilières (ACVM) au Canada, à l'instar de la SEC ont publié en 2017 "l'Avis multilatéral 51-347 " qui oblige les émetteurs à informer les investisseurs des cyberrisques importants et à déclarer tout incident de cybersécurité jugé matériel pour l'entreprise, à savoir : les formes et les sources de l'exposition à la cybersécurité, le niveau d'exposition et les motifs qui le sous-tendent, la capacité de réaction de l'émetteur au risque, les conséquences possibles d'une cyberattaque et les incidents importants antérieurs, ou la série d'incidents, liés à la cybersécurité et leurs effets sur les risques liés à la cybersécurité de l'émetteur. De ce fait, la divulgation est une pratique fortement encouragée, voire exigée pour toutes les sociétés canadiennes ouvertes.

La littérature sur la divulgation en matière de cybersécurité se construit encore, vu qu'il y a jusqu'ici un nombre limité de recherches empiriques traitant du sujet à notre connaissance. De plus, comme les exigences en matière de divulgation sont plus poussées aux États-Unis depuis un certain temps, la majorité des recherches scientifiques publiées jusqu'ici traitent de la cybersécurité dans le contexte américain. À titre d'illustration, Mazumder et Hossain (2023) et Sari et al., (2024) recensant la littérature effectuée jusqu'ici sur la divulgation en matière de cybersécurité, remarquent que les USA est le contexte le plus étudié.

Par ailleurs, certaines études empiriques réalisées au Canada, comme celles de Smaili et al. (2023) et Héroux et Fortin (2024), ont contribué à mettre en évidence le rôle du conseil d'administration dans la divulgation des informations de cybersécurité. Cependant, elles s'appuient principalement sur des périodes d'analyse assez anciennes (de 2014 à 2018). Étant donné l'évolution considérable des enjeux liés à la cybersécurité au cours des dernières années, les pratiques de divulgations ont fort probablement à leur tour évolué. Il est donc pertinent de contribuer à la littérature sur le sujet en proposant une analyse utilisant des données plus récentes dans le contexte canadien.

Comme mentionné, le contexte canadien est important. C'est dans cette perspective et soutenu par les arguments avancés dans les paragraphes précédents que nous avons décidé de pousser des

réflexions sur la présente question de recherche : **« Quels sont les déterminants de la divulgation en matière de cybersécurité effectuée par les entreprises cotées ?**»

La motivation principale de cette étude, en répondant à cette question, est de compléter la littérature existante qui est peu développée et qui continue de se construire. L'objectif poursuivi est d'investiguer les facteurs qui influencent la divulgation en matière de cybersécurité par les entreprises canadiennes cotées en bourse en s'appuyant simultanément sur la théorie des ressources et la théorie du signal. La première permet d'identifier les caractéristiques du conseil à une ressource stratégique qui améliore la divulgation de cybersécurité, conférant un avantage concurrentiel à l'entreprise. La seconde met en évidence l'importance de la composition du conseil d'administration comme un signal d'engagement face aux enjeux de cybersécurité, tout en réduisant l'asymétrie d'information grâce au partage d'informations pertinentes avec les parties prenantes (Héroux et Fortin, 2024 ; Smaili *et al.*, 2023).

Notre étude s'appuie sur un échantillon de 180 entreprises-années de la S&P/TSX 60 pour les années 2021 à 2023. Elle adopte une approche mixte combinant l'analyse de contenu automatisé via Nvivo pour mesurer la divulgation de cybersécurité dans les rapports annuels et utilise un modèle de régression logistique et linéaire multiple pour son analyse.

Les résultats obtenus apportent des preuves quant à l'influence des caractéristiques du conseil d'administration sur la divulgation. Il s'agit spécifiquement de son indépendance et de l'expertise en technologies de l'information de ses membres qui ressortent positifs et significatifs à l'issue de test statistique. Par conséquent, les conseils dotés de membres indépendants et possédant une compétence spécifique (TI, cybersécurité, ou autres liées aux TI…) sont plus disposés à communiquer davantage d'informations sur la cybersécurité. Par ailleurs, les résultats indiquent également que la diversité de genre du conseil est un déterminant du choix de publier (ou pas) de l'information concernant la cybersécurité, tandis qu'elle n'a pas d'influence sur le volume de l'information publiée. En revanche, contrairement aux prédictions, la taille du conseil ainsi que la rentabilité et la taille de l'entreprise ne ressortent pas significatives. Autrement dit, ces facteurs ne sont pas des déterminants de la divulgation en matière de cybersécurité.

Ce mémoire apporte une triple contribution à la littérature en complétant les recherches antérieures.

D’abord sur le plan théorique, il contribue à l’enrichissement de la littérature sur la divulgation de cybersécurité en mobilisant conjointement la théorie des ressources et celle du signal pour étudier les déterminants de cette divulgation dans le contexte canadien.

Ensuite, sur le plan méthodologique, il propose une approche à la fois qualitative (utilisation d’un instrument de codage quanti-quali) et quantitative (tests de régression) dans le but d’atteindre l’objectif de recherche.

Enfin, sur le plan pratique, il met en évidence l’importance de la divulgation réactive pour se conformer aux réglementations, ou proactive, en dépassement des exigences réglementaires, pour renforcer la confiance des parties prenantes et limiter les impacts financiers des cyberattaques

Le présent document sera structuré comme suit : le chapitre 1 sera consacré à la revue de littérature sur la divulgation en matière de cybersécurité et le chapitre 2 traitera du cadre théorique mobilisé pour soutenir cette recherche. Ensuite, le chapitre 3 développera les hypothèses retenues pour l'étude et le chapitre 4 décrira la méthodologie adoptée pour procéder à l’analyse. Enfin, le chapitre 5 discutera des résultats empiriques de l'étude à la lumière de la littérature existante.

CHAPITRE 1
REVUE DE LITTÉRATURE

Dans ce chapitre, nous passerons en revue la littérature existante afin d'y identifier les apports majeurs, les polémiques et les manques, qui nous permettront à terme de situer notre recherche dans son champ académique.

1.1 Cadre réglementaire de la divulgation de cybersécurité

Les entreprises sont tenues de divulguer certaines informations en raison des lois, des normes comptables et des exigences réglementaires. Ces informations sont qualifiées de « divulgation obligatoire ». Cependant, les entreprises peuvent également choisir de divulguer des informations de manière volontaire, au-delà des obligations formelles. Cette divulgation est appelée « divulgation volontaire ». Elle vise à réduire l'asymétrie d'information entre l'entité et ses parties prenantes en fournissant des informations additionnelles et pertinentes pour influencer les perceptions (C. Radu, SCO8211 - Communication de l'information financière et organisationnelle, ESG UQAM, hiver 2024).

La divulgation de cybersécurité peut se situer entre ces deux extrêmes en tant que divulgation attendue, car n'étant pas tout à fait obligatoire ou volontaire. En effet, en matière de cybersécurité, les obligations de divulgation reposent encore principalement sur des directives et des avis interprétatifs publiés par les autorités réglementaires ; ce qui laisse une marge de manœuvre aux entreprises dans la communication de ces informations.

1.1.1 Encadrement réglementaire de la divulgation de cybersécurité

La divulgation d'informations constitue un moyen pour les entreprises de répondre aux attentes de leurs parties prenantes. Par conséquent, les sociétés adoptent des stratégies de divulgation en matière de cybersécurité afin de satisfaire les attentes de leurs parties prenantes en termes d'informations sur leur cybersécurité. Cependant, en raison de l'importance croissante de la cybersécurité, les organismes de réglementation, tels que la Securities and Exchange Commission

(SEC) aux États-Unis et l'Autorité canadienne en valeurs mobilières (ACVM) au Canada, ont également pris un intérêt pour ce sujet. Leur objectif est de standardiser les pratiques de divulgation.

1.1.1.1 Encadrement aux États-Unis (SEC)

La Securities and Exchange Commission (SEC) est l'organisme fédéral américain qui réglemente et contrôle les marchés financiers. Elle définit la cybersécurité comme « l'ensemble des technologies, des processus et des pratiques conçus pour protéger les réseaux, les systèmes, les ordinateurs, les programmes et les données contre les attaques, les dommages ou l'accès non autorisé » (SEC, 2011). Pour s'assurer que les entreprises fournissent aux investisseurs des informations pertinentes concernant les menaces et incidents liés à la cybersécurité, la SEC a mis au point en 2011 des directives qui ont subi des modifications en 2018 et récemment en 2023.

- Directives de la SEC en 2011

Compte tenu de la dépendance des émetteurs vis-à-vis des technologies numériques, les risques de cybersécurité ont augmenté, entrainant une recrudescence des cyberincidents. Face à cela, la SEC a émis des directives qui invitent les entreprises cotées à divulguer les informations en temps voulu, complet et exact sur les risques et incidents qu'un investisseur raisonnable jugerait importants pour une décision d'investissement. La SEC rappelle « qu'il ne s'agit pas d'une règle, d'une réglementation ou d'une déclaration ». Selon ces directives :

- Les entreprises doivent évaluer leurs risques en cybersécurité et fournir des divulgations appropriées, en particulier si ces risques sont significatifs pour les investisseurs ;
- Les divulgations doivent inclure les principaux risques, les incidents passés significatifs, les impacts potentiels ainsi que les stratégies d'atténuation.
- Les entreprises doivent veiller à ne pas compromettre leur sécurité en divulguant des détails techniques sensibles.

Il faut souligner que ces directives étaient purement interprétatives (SEC, 2011), ce qui a conduit à des divulgations variées et souvent insuffisantes.

- Directives de la SEC en 2018

En réponse à la multiplication des cyberincidents et leurs impacts sur les entreprises, la SEC a mis à jour en février 2018 les directives de 2011 pour renforcer et élargir les attentes en matière de divulgation. Ainsi, l'accent est mis sur :

- Une fois encore, les risques et incidents de cybersécurité, dans le sens où les divulgations sur ces derniers doivent inclure les coûts de remédiation, les pertes de revenu, les litiges, les dommages à la réputation et les impacts sur la compétitivité ;
- Les contrôles et les procédures de divulgation qui doivent être mis en place par les entreprises pour identifier et évaluer les risques et incidents de cybersécurité et pour s'assurer que les informations pertinentes sont communiquées aux responsables de la divulgation ;
- L'interdiction du délit d'initié dans le sens où les dirigeants et entités de l'entreprise ne doivent pas négocier des titres de l'entreprise en possession d'informations non publiques importantes sur les incidents de cybersécurité ;
- Le conseil d'administration doit démontrer son implication dans la supervision des menaces informatiques et sa collaboration avec la direction à cet égard.
- La divulgation équitable (Fair disclosure FD) : une nouvelle règle de divulgation des émetteurs mis au point par la SEC qui traite de la communication sélective. Il interdit la divulgation partielle d'informations importantes non publiques. De ce fait, quand un émetteur divulgue ces informations à certains investisseurs ou intervenants du marché, il se doit également de les rendre publiques. Si la révélation est délibérée, elle doit intervenir simultanément ; si elle est fortuite, elle doit être rendue publique rapidement afin de garantir une diffusion étendue et équitable. (*Selective Disclosure and Insider Trading*, 2023)
- Les divulgations via les rapports périodiques : les entreprises sont tenues de déposer des formulaires 10-K pour communiquer des informations spécifiques sur une base régulière et continue. De plus, la SEC encourage les émetteurs à continuer de divulguer rapidement les informations à travers les formulaires 8-K et 6-K. Les différents formulaires présentent une certaine particularité qu'il convient de distinguer. Ainsi, on désigne par :
    - Formulaire 10-K: un rapport déposé chaque année par une société déclarante auprès de la (SEC) afin de divulguer des informations commerciales et financières complètes sur la société au cours du dernier exercice clos (*Form 10-K | Practical Law*, s. d.).

- Formulaire 8-K : un rapport courant qui sert à divulguer rapidement tout événement majeur dont les actionnaires doivent être informés. Il doit être déposé dans les quatre jours ouvrables suivant l'événement (*Form 8-K | Investor.gov*, s. d.)
- Formulaire 6-K : un rapport qui permet aux entreprises étrangères privées (non américaines) enregistrées auprès de la SEC de transmettre toute information importante rendue publique dans leur pays d'origine. Grâce à lui, les investisseurs américains ont accès aux mêmes informations que les investisseurs locaux de l'entreprise. Il est déposé dès qu'une info importante est publiée dans le pays d'origine (Understanding SEC Form 6K, 2025)

➢ Directives de la SEC en 2023

Suites aux premières directives de la SEC, Li et al (2018) ont examiné d'une part l'utilité des divulgations des risques de cybersécurité dans les rapports financiers des entreprises et, d'autre part l'impact des directives de divulgation de la cybersécurité de la SEC sur les pratiques de divulgation des entreprises. Les auteurs trouvent que les directives de la SEC ont entrainé des divulgations de risques de cybersécurité génériques. Ils soutiennent que ce résultat découlerait de l'ambiguïté des directives et des lettres de commentaires envoyées par la SEC pour forcer les entreprises à divulguer des informations sur la cybersécurité.

Face aux pratiques incohérentes et insuffisantes de divulgation des entreprises et à la croissance continue des cyberincidents, la SEC a publié en 2023 ses directives actualisées dans le but de standardiser et d'améliorer les divulgations de risques et d'incidents en matière de cybersécurité. Par conséquent, « la SEC a indiqué que, selon elle, les directives précédentes n'avaient pas suffisamment permis d'améliorer les pratiques en ce qui concerne la communication d'information sur la cybersécurité et qu'il était nécessaire de rendre certaines pratiques obligatoires pour que les investisseurs soient en mesure de localiser, d'interpréter et d'analyser l'information dont ils ont besoin » (Comerford et MacDougall, 2023, p. 2). Ainsi, les nouvelles directives sont résumées dans le tableau suivant :

Tableau 1.1 Récapitulatif des directives de la SEC 2023

Document	**Information à fournir**
Déclaration des incidents	Les émetteurs nationaux américains doivent déclarer sur le formulaire 8-K tout incident lié à la cybersécurité qu'ils déterminent comme important et décrire les aspects importants i) de sa nature, de sa portée et de sa chronologie et ii) de son incidence ou de l'incidence qu'il est raisonnablement susceptible d'avoir.
Rapports courant sur formulaire 8-K	Le formulaire 8-K doit être déposé dans les quatre jours ouvrables suivant la détermination de l'importance de l'incident, mais le dépôt peut être retardé si le procureur général des États-Unis détermine qu'une déclaration immédiate soulèverait un risque substantiel pour la sécurité nationale ou la sécurité publique. Le délai de quatre jours ouvrables doit être respecté, même si certains éléments d'information à fournir n'ont pas été déterminés ou n'étaient pas disponibles au moment du dépôt du formulaire 8-K. Un formulaire 8-K modifié doit être déposé une fois que ces éléments d'information ont été déterminés ou sont devenus disponibles.
Rapports courant sur formulaire 6-K	Les EPE[3] doivent fournir sur le formulaire 6-K l'information sur les incidents importants liés à la cybersécurité qu'elles déclarent ou rendent publics d'une autre manière dans un territoire étranger, aux bourses de valeurs ou aux porteurs de titres.

[3] EPE signifie : Émetteurs privés étrangers

Informations à fournir dans le rapport annuel	
Rapport annuel sur formulaire 10-K	
Information sur les risques liés à la cybersécurité	Les émetteurs nationaux américains doivent décrire les processus qu'ils mettent en œuvre pour évaluer, repérer et gérer les risques importants liés aux cybermenaces, et indiquer si ces risques ont eu ou sont raisonnablement susceptibles d'avoir une incidence importante sur leur stratégie commerciale, leurs résultats d'exploitation ou leur situation financière.
Gouvernance liée à la cybersécurité	Les émetteurs nationaux américains doivent décrire comment leur conseil d'administration surveille les risques liés aux menaces informatiques et le rôle du leadership dans l'évaluation et la gestion des risques majeurs associés à ces menaces.
Rapport annuel sur formulaire 20-F	Les EPE doivent décrire les mécanismes par lesquels le conseil d'administration surveille les risques liés aux cybermenaces, de même que le rôle de la direction dans l'évaluation et la gestion des risques importants liés aux cybermenaces.

Source: Comerford et MacDougall (2023)

1.1.1.2 Encadrement au Canada (Autorité canadienne en valeurs mobilières ACVM)

Au Canada, la réglementation du commerce des valeurs mobilières est sous la juridiction des provinces et territoires. Pour synchroniser leurs efforts et standardiser les règles à l'échelle nationale, ces entités ont mis en place les Autorités canadiennes en valeurs mobilières (ACVM)[4],

[4] https://www.autorites-valeurs-mobilieres.ca/nouvelles/les-acvm-annoncent-lordre-du-jour-de-la-table-ronde-sur-la-cybersecurite/ Consulté le 2025-02-03

dont le but est de mettre en œuvre un cadre réglementaire uniforme à travers tout le pays. Elles poursuivent un triple objectif à savoir : la protection des investisseurs, le maintien de marchés équitables, efficients et transparents, la réduction du risque systémique.

Les Autorités canadiennes en valeurs mobilières ont publié le 19 janvier 2017 l'Avis multilatéral 51-347 du personnel des ACVM intitulé *Information sur les risques et les incidents liés à la cybersécurité*. Ce rapport vise à présenter les résultats obtenus à la suite de l'analyse de l'information fournie par les entreprises cotées en bourse sur les risques et incidents liés à la cybersécurité. Il en ressort que 146 émetteurs sur 240 ont reconnu la cybersécurité comme faisant partie des facteurs de risques présents dans leurs divulgations. Face à l'urgence de la situation, les ACVM s'attendent à ce que les émetteurs communiquent aux investisseurs des informations sur les cyberrisques significatifs, ainsi que tout incident de cybersécurité jugé matériel pour l'entreprise. Cette divulgation doit inclure les types et les sources des expositions à la cybersécurité, le niveau et les raisons de cette exposition, la capacité de l'émetteur à gérer ces risques, les conséquences potentielles d'une cyberattaque, ainsi que les incidents majeurs antérieurs ou une série d'incidents et leurs répercussions sur les risques liés à la cybersécurité (Anton *et al.*, 2017). Plus spécifiquement :

- Les émetteurs devraient divulguer les informations importantes et intrinsèques à leur situation et éviter les discours génériques ;
- Les émetteurs ne doivent pas divulguer des détails sur leur stratégie en matière de cybersécurité ou leur vulnérabilité aux cyberattaques qui pourraient compromettre leur sécurité ;
- Les émetteurs doivent évaluer la probabilité qu'une atteinte survienne et l'ampleur prévue de son incidence pour déterminer l'importance relative des risques liés à la cybersécurité ;
- L'information sur les risques liés à la cybersécurité doit être adaptée à la situation spécifique de l'émetteur, en tenant compte des facteurs soulevés par l'OICV ;
- Les émetteurs doivent traiter les questions de gouvernance, en mentionnant le nom du comité ou de la personne responsable de leur stratégie en matière de cybersécurité et de gestion des risques.

- Les émetteurs doivent évaluer si un cyberincident est important et doit être communiqué conformément à la législation en valeurs mobilières. L'importance relative d'un incident dépend de son contexte et de ses conséquences.

Les ACVM insistent sur la nécessité pour les entreprises d'améliorer la qualité et la précision de leurs informations sur la cybersécurité. Pour les prochaines étapes, elles continueront de surveiller les pratiques des entreprises et de suivre l'évolution des divulgations sur les cyberincidents (*CSA Multilateral Staff Notice 51-347 - Disclosure of cyber security risks and incidents*, 2017).

1.1.1.3 Répercussion des directives de la SEC et des ACVM pour les émetteurs canadiens

Dans les deux sous-sections précédentes, nous avons abordé les directives mises en place par les autorités nord-américaines (SEC et ACVM) pour régir la divulgation en matière de cybersécurité. Les entreprises canadiennes qui sont à la fois émettrices sur les bourses canadiennes et américaines sont, par conséquent, tenues de communiquer les informations de cybersécurité en se conformant à la fois aux directives de la SEC et des ACVM.

En vertu des lois canadiennes, et contrairement aux directives finales de la SEC qui imposent la divulgation d'un cyberincident dans le formulaire 8-K dans un délai de 4 jours, les entreprises canadiennes cotées à la bourse doivent déposer un communiqué dès qu'un cyberincident est jugé matériel. En outre, dans la mesure où les sociétés canadiennes sont inscrites sur les bourses américaines, elles devront déclarer rapidement à travers les formulaires 6-K, ces cyberincidents déjà publiés au Canada (Comerford et MacDougall, 2023). Ainsi, selon Comerford et MacDougall (2023), il est recommandé aux émetteurs canadiens de :

- Renforcer les contrôles et procédures de communication afin d'assurer une communication rapide des incidents à la haute direction et aux services juridiques ;
- Sensibiliser le conseil d'administration et la direction aux obligations d'information sur les incidents liés à la cybersécurité ;
- Mettre en place un comité dédié au sein du conseil d'administration disposant de l'expertise nécessaire pour superviser les questions de cybersécurité.

1.1.2 Divulgation volontaire

Outre les pratiques de divulgation réactives par les entreprises pour se conformer aux réglementations, elles procèdent également à la divulgation discrétionnaire ou volontaire d'informations. En général, les entreprises choisissent de divulguer volontairement les risques afin de réduire l'asymétrie d'information et renforcer la confiance des investisseurs quant à la gestion efficace des risques de l'entreprise (Elsayed et Hassanein, 2024). De plus, la déclaration volontaire des risques peut servir de signal à l'environnement commercial sur la capacité de l'entreprise à identifier, mesurer et gérer les risques Hassanein et Elsayed (2021) cité par Elsayed et Hassanein (2024).

D'après la littérature existante, il existerait un lien de complémentarité ou de substitution entre la divulgation obligatoire et volontaire des risques. En effet, Cordazzo *et al.* (2017) ont investigué si l'interaction entre la divulgation obligatoire et volontaire des risques est complémentaire ou substitutive sous différents régimes de réglementation des risques, notamment : Allemagne, États-Unis, Italie, France et Royaume-Uni, durant la période 2007-2010. Les résultats révèlent que, dans chaque juridiction de réglementation des risques, il existe un effet complémentaire entre la divulgation obligatoire et volontaire des risques. Cela signifie que les entreprises ont tendance à compléter les informations obligatoires sur les risques par des divulgations volontaires. Les auteurs indiquent que leurs résultats sont contradictoires à leurs homologues Gigler et Hemmer (1998), Stocken (2000), Lundholm (2003) et Einhorn (2005), qui mettent en évidence un effet de substitution entre la divulgation obligatoire et volontaire des risques.

1.1.2.1 Facteurs influenceurs de la divulgation volontaire des risques

La divulgation volontaire des risques, comme mentionné précédemment, fait référence à la divulgation discrétionnaire d'informations de la part des entreprises pour compléter les points non couverts par la divulgation obligatoire. Il se trouve que, dans la littérature afférente, il existe des facteurs testés empiriquement et qui expliquent la décision des entreprises de divulguer de façon volontaire sur les risques.

Par exemple, Elshandidy *et al.* (2013) a examiné comment les niveaux de risque des entreprises influencent la divulgation agrégée, volontaire et obligatoire des risques dans les rapports annuels des entreprises cotées non financières au Royaume-Uni. Leurs résultats indiquent que les entreprises avec des niveaux élevés de risques systématiques, de financement et de rendements ajustés au risque sont plus susceptibles de divulguer des informations sur les risques de manière volontaire et agrégée. Ensuite, les entreprises ayant une grande taille, un rendement élevé des dividendes et une indépendance du conseil d'administration ont tendance à fournir plus de divulgations volontaires de risque. En revanche, une grande volatilité des rendements du marché réduit la propension des entreprises à divulguer volontairement des informations sur les risques.

Récemment, toujours dans le contexte britannique, Elsayed et Hassanein (2024) ont étudié l'impact de la gouvernance au niveau de l'entreprise sur la divulgation volontaire des risques et la pertinence informative de cette divulgation pour la valeur de l'entreprise. Leurs résultats confirment ceux de Elshandidy *et al.* (2013) quant à l'influence de l'indépendance du conseil d'administration. Cependant, selon eux, les conseils de grande taille avec une participation managériale élevée divulguent moins. Les résultats d'Elgammal et al. (2018), issus de l'étude sur l'impact de la gouvernance d'entreprise sur la divulgation des risques et des informations prospectives dans les rapports annuels des entreprises qatariennes de 2008 à 2014, s'alignent avec ceux d'Elshandidy et al. (2013) et d'Elsayed et Hassanein (2024). Ils confirment l'influence positive de l'indépendance du conseil d'administration et l'influence négative de sa taille sur la divulgation volontaire des risques.

1.1.2.2 Pertinence de la divulgation volontaire des risques pour les marchés des capitaux

Les entreprises en divulguant volontairement les risques veulent réduire l'asymétrie d'information entre elles et leurs parties prenantes et envoyer des signaux positifs aux investisseurs quant à la gestion des risques. Smaili et al (2023) souligne que « sur la base de la théorie des signaux (Akerlof, 1978), la divulgation de bonnes nouvelles est une opportunité pour le conseil d'administration et la direction de signaler que l'entreprise est en bonne position et sait gérer les risques ».

Plusieurs études ont mis en évidence l'impact positif de la divulgation volontaire en matière de risque sur la valeur de l'entreprise. Par exemple, Abdullah *et al* (2015) ont examiné à travers des

tests statistiques multivariés l'effet de la divulgation volontaire de la gestion des risques sur la valeur de l'entreprise. Ils ont trouvé que la divulgation volontaire de la gestion des risques est positivement et significativement liée à la valeur de l'entreprise, ce qui suggère que les investisseurs tendent à percevoir plus favorablement les entreprises qui communiquent davantage sur la gestion de leurs risques. De plus, Elsayed et Hassanein (2024) trouvent à leur tour que la divulgation volontaire des risques est associée à une meilleure valorisation des entreprises par les investisseurs, particulièrement dans les entreprises ayant un plus grand nombre d'administrateurs indépendants, une participation managériale plus faible et de grands comités d'audit.

L'étude de Al-Maghzom *et al*. (2017) visait à examiner la relation entre les niveaux de divulgation volontaire des risques et la valeur de l'entreprise dans les banques saoudiennes cotées. Les résultats suggèrent l'existence d'une association positive significative entre les niveaux de divulgation des risques et la valeur de l'entreprise. Autrement dit, les banques qui divulguent davantage d'informations sur les risques ont tendance à présenter une valeur d'entreprise plus élevée. Les auteurs expliquent que cette relation pourrait être liée au fait que la divulgation des risques est perçue par les investisseurs comme un signe de bonne gestion, de transparence et de responsabilité. Cela pourrait renforcer la confiance des investisseurs et des parties prenantes, et être associé à une meilleure performance financière.

Dans une étude ultérieure, Harymawan et Rahmawati (2022) ont employé le logarithme naturel de la capitalisation boursière comme indicateur de la valeur de l'entreprise. Ils ont examiné l'impact de la divulgation proactive de la gestion des risques et de la présence d'un comité de gestion des risques sur la valeur de l'entreprise. Ils trouvent que la divulgation volontaire de la gestion des risques positivement et significativement associée à la valeur de l'entreprise. En d'autres termes, les entreprises qui publient plus d'informations sur la gestion de leurs risques ont tendance à avoir une valeur de marché plus élevée. En outre, les auteurs soulignent que la divulgation volontaire de la gestion des risques est perçue positivement par les investisseurs parce qu'elle réduit l'asymétrie de l'information. Ainsi, lorsque les entreprises divulguent plus d'informations sur la gestion des risques, cela rassure les investisseurs sur la capacité de l'entreprise à gérer les incertitudes et à protéger leurs investissements. Cela conduit à une augmentation de la valeur perçue de l'entreprise.

Toutefois, en dehors de ces études qui mettent en lumière les effets positifs de la divulgation volontaire sur la valeur de l'entreprise et sur la perception des investisseurs, la littérature souligne que ces effets ne sont pas systématiquement positifs dans le sens où les informations peuvent être manipulées à des fins stratégiques. En effet, en raison de nature discrétionnaire, les dirigeants peuvent choisir le moment, le niveau et la nature des informations qu'ils divulguent en fonction de leurs propres incitations (Verrecchia, 2001). Dans cette perspective, la divulgation volontaire ne vise pas seulement à informer les investisseurs, mais peut aussi être utilisée stratégiquement pour influencer la perception du marché.

De plus, Healy et Palepu (2001) expliquent que les décisions de divulgation des entreprises sont influencées par plusieurs facteurs, tels que les incitations managériales, les coûts liés à la divulgation ou encore la concurrence, ce qui peut conduire à une divulgation sélective de l'information.

De récentes études sur la cybersécurité corroborent le caractère stratégique de la divulgation proactive. Par exemple, d'après Vo et Pham (2025), les sociétés confrontées à un risque élevé de cybermenaces ont tendance à publier plus de prévisions financières pour apaiser les inquiétudes des investisseurs. Cependant, ces prévisions sont généralement moins précises et fiables. Cela suggère que la divulgation volontaire peut également servir à manipuler l'opinion des investisseurs plutôt qu'à transmettre des informations complètes et exactes. Ainsi, la littérature indique que la divulgation proactive peut renforcer l'environnement informationnel des marchés et, dans certaines circonstances, refléter des comportements plus stratégiques et opportunistes chez les dirigeants.

1.2 Facteurs déterminants de la divulgation en matière de cybersécurité

Compte tenu de l'encadrement réglementaire qui incite les entreprises à communiquer certaines informations liées à la cybersécurité, ainsi que des pratiques de divulgation volontaire qu'elles adoptent, certains auteurs se sont donné comme objectif d'explorer les facteurs qui influencent ou non la divulgation en matière de cybersécurité par les entreprises. Ces études ont été réalisées dans différents contextes avec différentes méthodes d'analyse et leurs résultats se rejoignent ou se contredisent quant à l'impact de certains facteurs.

De façon globale, Sari *et al.* (2024) ont réalisé une revue systématique en analysant des articles de diverses revues internationales dans le but d'identifier les facteurs qui influencent les divulgations de cybersécurité. À la lumière de cette analyse, on constate que la taille du conseil d'administration, son indépendance, la diversité au sein du conseil d'administration, les actionnaires institutionnels, les actionnaires étrangers, cyberincidents antérieurs, les violations par les pairs, l'attention du public, les dépenses en capital, l'actif incorporel, la taille de l'entreprise, la croissance de l'entreprise et l'endettement de l'entreprise sont les facteurs déterminants des divulgations en matière de cybersécurité. Étant donné que leur étude se résumait à une revue systématique, il convient de fournir une explication plus en détails de l'influence de ces différents facteurs.

1.2.1 L'impact des violations de données et des directives de la SEC sur la divulgation de cybersécurité

Microsoft définit une violation de données[5] comme « la conséquence d'un accès non autorisé aux informations, au réseau ou aux appareils d'une organisation, suite à une cyberattaque, à des menaces internes ou à une erreur humaine ». La littérature a constaté que, dans la plupart des cas, les entreprises divulguent davantage ou moins sur leur cybersécurité à la suite des violations de données qu'elles auraient subies.

En effet, avec la publication des premières directives de la SEC en 2011 et 2018, Li *et al* (2018) ont examiné l'utilité des facteurs de risque liés à la cybersécurité divulgués dans les dépôts 10-K et leur relation avec les incidents de cybersécurité futurs. Ils affirment qu'avant les lignes directrices de la SEC, la présence et la longueur des divulgations des risques de cybersécurité étaient liées aux incidents futurs. Ce qui signifie que les entreprises qui divulguaient des risques de cybersécurité étaient plus sujettes aux incidents de cybersécurité par la suite. De plus, les auteurs trouvent qu'après l'introduction de la SEC, l'association et entre la présence des divulgations et des cyberincidents devient insignifiants ; ce qui s'expliquerait par le fait que les entreprises ont commencé à divulguer les risques de cybersécurité indépendamment de leur niveau réel de risque. En outre, ils mentionnent l'augmentation générale de la longueur des divulgations après

[5] https://www.microsoft.com/fr-ca/security/business/security-101/what-is-data-protection
Consulté le 2025-02-11

l'introduction des lignes directrices de la SEC et la diminution de leur nature informative, car les entreprises publieraient des divulgations plus longues pour se conformer aux exigences réglementaires, même si elles ne font pas face à des risques de cybersécurité substantiels.

Plus tard en 2020, l'étude de Gao et al. (2020) révèle que les entreprises ayant déjà été victimes de cyberincidents divulguent davantage sur les risques dans le but de rassurer les parties prenantes et de se protéger de futurs incidents. Comme Li *et al* (2018), ils trouvent que la longueur des divulgations de risques de cybersécurité a augmenté significativement après la publication des directives de la SEC. Cependant, ils indiquent que la lisibilité des divulgations a diminué, entrainant des divulgations de plus en plus difficiles à lire au fil du temps.

Par la suite, D'Arcy *et al* (2022) ont investigué l'impact de la pression publique suite à l'annonce de violations de données par les entreprises et l'impact de la pression institutionnelle résultant des violations de données par les pairs de l'industrie. Ainsi, ils distinguent deux types de violations de données, à savoir les violations externes et les violations internes. Selon eux, les entreprises ont tendance à divulguer plus d'informations sur la cybersécurité pour maintenir la légitimité auprès des investisseurs après une violation externe, car celle-ci conduit à une forte pression publique. En revanche, les entreprises divulguent moins d'informations après une violation interne, car elles sont plus susceptibles d'être tenues responsables et, par conséquent, jouent la carte de la prudence pour ne pas nuire à leur réputation. Les auteurs mentionnent également les violations par les pairs de l'industrie qui entrainent habituellement moins de divulgations, sauf dans les cas où l'entreprise victime subit également une violation externe.

1.2.2 L'impact des caractéristiques du conseil d'administration sur la divulgation de cybersécurité

La SEC, dans ses directives, met en lumière l'importance du rôle de surveillance du conseil d'administration vis-à-vis des risques de cybersécurité. Ainsi, pour remplir efficacement ce rôle, le conseil d'administration se doit de respecter un certain nombre de caractéristiques. De ce fait, la littérature a recensé plusieurs études qui ont examiné l'influence des caractéristiques du conseil d'administration sur la divulgation en matière de cybersécurité. Bien que la plupart des études se

rejoignent dans leurs conclusions, il existe néanmoins certaines d'entre elles qui se contredisent quant à l'impact de certains facteurs.

1.2.2.1 La taille du conseil d'administration

La taille du conseil d'administration fait référence au nombre d'administrateurs composant le conseil. Plusieurs auteurs dans leurs études ont prédit une relation positive entre la taille du conseil et la divulgation en matière de cybersécurité. Mais, force est de constater que ce facteur n'a en réalité pas été confirmé empiriquement comme influençant cette divulgation dans la plupart des études.

À titre d'illustration, Mazumder et Hossain (2023) et Smaili et al (2023) cherchaient à savoir si la taille du conseil d'administration influençait la divulgation de cybersécurité dans un contexte bangladais (pour le premier) et canadien (pour le second). Ils ont émis l'hypothèse que la taille du conseil d'administration est positivement et significativement associée à la divulgation en matière de cybersécurité. Pour Mazumder et Hossain (2023) cette relation positive trouve son essence dans le fait que, selon la théorie de l'agence et la théorie des ressources, un conseil d'administration plus grand est associé à une surveillance plus efficace des actions managériales et à une diversité d'expertise et de connaissances transversales. D'après Smaili *et al* (2023), cette hypothèse suggère que les conseils d'administration plus grands, avec une diversité d'expertises et d'expériences, sont plus susceptibles de divulguer des informations sur la cybersécurité. Sur la base de ces arguments, les auteurs, après analyse statistique, ont dû rejeter cette hypothèse, car leurs résultats n'ont pas pu confirmer une relation positive et significative de la taille du conseil sur la divulgation de cybersécurité. Smaili *et al* (2023) expliquent cela par le manque d'expertise spécifique à la cybersécurité chez la plupart des administrateurs.

Tout récemment, Alodat *et al.* (2024) ont exploré l'influence des caractéristiques du conseil d'administration sur la divulgation de la cybersécurité des entreprises cotées à la Bourse de Londres. L'étude a été réalisée dans le contexte britannique où les auteurs mentionnent que la divulgation de la cybersécurité est volontaire, ce qui rend l'étude de ces caractéristiques encore plus pertinentes pour comprendre les pratiques de divulgation. En ce qui concerne l'influence de la taille du conseil d'administration sur la divulgation de cybersécurité, les auteurs trouvent une relation positive et

significative. Ils soutiennent que les entreprises dont le conseil d'administration est plus grand fournissent davantage d'informations en matière de cybersécurité. De plus, selon la théorie de l'agence, ce résultat est corroboré par les conseils d'administration plus grands qui mettent en œuvre des mesures de contrôle efficaces pour réduire les risques. Ces résultats contrastent avec ceux obtenus dans d'autres contextes empiriques, notamment par Mazumder et Hossain (2023) et Smaili *et al* (2023), qui ne trouvent pas de relations significatives entre la taille du conseil et la divulgation de cybersécurité. Ainsi, la littérature ne semble pas parvenir à un consensus quant à l'influence de ce facteur. Ce qui suggère que son impact peut varier selon le contexte institutionnel et les caractéristiques de l'échantillon étudié.

1.2.2.2 L'indépendance du conseil d'administration

Selon CPA Canada[6], « un administrateur est dit indépendant s'il n'a aucun lien direct ou indirect important avec la société, qui, de l'avis du conseil d'administration, pourrait raisonnablement l'empêcher d'exercer un jugement indépendant ». De ce fait, l'indépendance est une caractéristique incontournable d'un conseil d'administration efficace. Étant donné que le conseil doit jouer un rôle de surveillance des risques de cybersécurité, il est normal que ses caractéristiques, notamment l'indépendance, aient un impact sur la divulgation. Il est important de noter que plusieurs études ont été réalisées sur le sujet. La grande majorité d'entre elles montrent qu'il existe une relation positive entre l'indépendance du conseil et la divulgation de cybersécurité.

D'abord dans le contexte canadien, Smaili *et al.* (2023) avec une étude réalisée sur un échantillon de 60 grandes entreprises cotées à la Bourse de Toronto, formant l'indice S&P/TSX60 sur période de 4 ans donnant un total de 300 observations ont trouvé que l'indépendance des membres du conseil a un impact positif sur le volume de cette divulgation de cybersécurité. Les auteurs expliquent que les membres indépendants du conseil d'administration, qui agissent comme un mécanisme de gouvernance et de surveillance, augmentent considérablement la divulgation des risques de cybersécurité dans les états financiers de l'entreprise. Ces résultats ont été reconfirmés plus tard par Héroux et Fortin (2024) qui ont réalisé une étude sur l'association entre les

[6] https://www.cpacanada.ca/fr/-/media/site/business-and-accounting-resources/docs/20-questions-que-les-administrateurs-devraient-poser-sur-constitution-et-le-maintien-dun-conseil-dadministration-efficace-fr-juillet-r2-00304.pdf?rev=6eb2fd19fb8e444f9dfeab4f672ecdb4

caractéristiques des différents conseils d'administration et l'étendue de la divulgation globale de la cybersécurité et ses aspects individuels, avec un échantillon de 250 plus grandes entreprises canadiennes listées sur l'indice S&P/TSX composite. Les auteurs ont effectué une analyse de contenu à l'aide d'une grille de codage de 40 items développée pour mesurer la divulgation de la cybersécurité, basée sur les lignes directrices des régulateurs financiers. Cette analyse a été soutenue par des régressions Tobit pour tester les associations entre les caractéristiques des conseils d'administration et l'étendue de la divulgation de la cybersécurité. En plus des rapports annuels utilisés dans la plupart des études, les auteurs ont collecté leurs données à partir de formulaires d'information annuels (FIA), et des circulaires de procuration disponibles publiquement. Leurs résultats indiquent que l'indépendance du conseil est positivement associée à l'étendue de la divulgation de la cybersécurité. Cela dit, les membres indépendants apportent une variété de perspectives et de connaissances qui peuvent influencer positivement la divulgation.

Ensuite, dans le contexte britannique, Alodat *et al.* (2024) avec un total de 2250 observations d'entreprises britanniques cotées à la Bourse de Londres pour la période de 2011 à 2020, trouvent une relation significative et positive entre l'étendue de la divulgation de cybersécurité et l'indépendance du conseil. Ils soutiennent que les conseils d'administration indépendants favorisent la transparence et la bonne gouvernance, réduisent l'asymétrie de l'information, fournissent davantage d'informations sur les risques de cybersécurité et réduisent les problèmes d'agence.

Enfin, dans le contexte bangladais, avec une étude sur un échantillon de 30 banques commerciales cotées donnant un total de 210 observations annuelles pour la période de 2014 à 2020, Mazumder et Hossain (2023) ont trouvé qu'il existe une relation positive significative entre l'indépendance du conseil d'administration et la divulgation volontaire de la cybersécurité. Ainsi, ils soutiennent que les banques ayant un pourcentage plus élevé de directeurs indépendants dans leur conseil d'administration fournissent plus d'informations sur la cybersécurité.

1.2.2.3 La diversité de genre au sein du conseil d'administration

On entend par diversité de genre la proportion de femmes administratrices siégeant au conseil d'administration. Cette caractéristique du conseil d'administration a longuement été étudiée par les

auteurs dans différents contextes. Ici il est question de l'impact de la diversité de genre au conseil sur la divulgation en matière de cybersécurité. La majorité des études présentées dans la littérature indique une relation positive.

En effet, Radu et Smaili (2022) ont examiné comment la composition de genre du conseil peut influencer la divulgation de cybersécurité, en se basant sur un échantillon d'entreprises cotées à l'indice S&P/TSX 60, entre 2014 et 2018. Leurs résultats indiquent qu'il existe une association positive entre la présence de femmes au sein du conseil d'administration et le niveau de divulgation de l'information sur la cybersécurité. Ainsi, selon ces auteurs, les entreprises avec des conseils plus diversifiés en termes de genre sont plus susceptibles de divulguer des informations pertinentes sur les risques de cybersécurité. Ils soulignent que cet impact positif est significatif si et seulement si le conseil d'administration compte au moins trois femmes soutenant ainsi la théorie de la masse critique. De ce fait, du point de vue des auteurs, la diversité de genre améliore l'efficacité du conseil d'administration en matière de gouvernance et de gestion des risques, ce qui conduit à une meilleure divulgation des risques de cybersécurité.

Mazumder et Hossain (2023) à leur tour, ont prédit l'existence d'une relation positive significative entre la diversité de genre au sein du conseil d'administration et la divulgation volontaire de la cybersécurité dans les banques commerciales cotées au Bangladesh. Leur prédiction s'est avérée exacte, confirmant ainsi les résultats de Radu et Smaili (2022). En effet, ils ont trouvé qu'une plus grande présence de femmes dans le conseil d'administration est associée à une divulgation volontaire de la cybersécurité plus élevée. Cela dit, les banques avec une plus grande diversité de genre dans leur conseil d'administration divulguent plus d'informations sur la cybersécurité.

De leur côté, Héroux et Fortin (2024) trouvent également que la présence de femmes au conseil est positivement associée à l'étendue de la divulgation de la cybersécurité. Ils soutiennent que les femmes directrices sont plus sensibles aux risques et aux responsabilités sociales, ce qui peut conduire à une meilleure divulgation.

Pour continuer, Kurnia et Ardianto (2024) ont poussé leur réflexion sure : comment la diversité de genre au sein des conseils d'administration influence-t-elle la divulgation de la cybersécurité dans le secteur bancaire indonésien, dans un contexte de gouvernance à deux niveaux ? Ils avaient pour

objectif d'explorer l'impact de la présence des femmes dans les conseils de surveillance et les équipes de direction sur la divulgation des risques de cybersécurité dans les banques indonésiennes, en tenant compte de la culture patriarcale dominante dans le pays. Avec un échantillon de 47 banques totalisant 376 observations sur 8 ans, les résultats montrent que la présence de femmes au sein du conseil d'administration augmente la divulgation de cybersécurité, tandis que la présence de femme au sein de l'équipe de direction a un effet significativement négatif sur cette divulgation. Les auteurs expliquent cet effet positif de la diversité sur la divulgation par le fait que les femmes au conseil de surveillance jouent un rôle crucial dans la surveillance et la fourniture de conseils sur la gestion des risques de cybersécurité. Concernant la masse critique, ils trouvent que la présence d'une ou deux femmes peut augmenter la divulgation de cybersécurité ; mais l'effet contraire se produit lorsque le nombre de femmes passe à trois. Ces résultats contredisent Radu et Smaili (2022) qui affirment que le nombre de femmes doit atteindre trois pour observer une relation positive. En outre, Kurnia et Ardianto (2024) expliquent l'effet négatif de la présence de femmes dans l'équipe de direction par le fait qu'elles sont souvent confrontées à des obstacles culturels et organisationnels qui limitent leur capacité à influencer positivement la divulgation de la cybersécurité.

Enfin, Alodat *et al.* (2024) s'attendant à une relation positive et significative entre la diversité et la divulgation de cybersécurité ont dû rejeter leur hypothèse, car les résultats indiquaient une relation positive, mais non significative entre la diversité de genre du conseil et l'étendue de cette divulgation. Ils soulignent que les femmes membres du conseil d'administration pourraient être plus réticentes à divulguer des informations sensibles sur les risques de cybersécurité pour éviter que ces informations ne tombent entre les mains des pirates. Ainsi, cette prudence pourrait limiter la divulgation de la cybersécurité.

Dans la majorité des contextes étudiés par les différents auteurs, il ressort que la présence de femmes administratrices influence positivement la divulgation en matière de cybersécurité. Ainsi, la diversité de genre constitue un paramètre non négligeable dans la composition du conseil d'administration vis-à-vis de son rôle de surveillance des risques de cybersécurité.

1.2.3 L'impact des facteurs organisationnels sur la divulgation en matière de cybersécurité

Les facteurs organisationnels désignent les caractéristiques qui définissent le fonctionnement, la structure et l'identité d'une entreprise. La littérature mentionne plusieurs facteurs incontournables qui définissent la structure d'une entité. Il en existe qui sont généralement utilisés par les chercheurs dans leurs études. Dans la plupart des études réalisées sur les divulgations, les facteurs organisationnels, notamment la taille de l'entreprise, la rentabilité, l'endettement, le secteur d'activité, sont utilisés comme variables de contrôle.

1.2.3.1 La taille de l'entreprise

De façon générale, la taille de l'entreprise peut définir l'étendue de la divulgation dans le sens où les grandes entreprises divulgueraient plus d'informations que les petites, car elles doivent satisfaire les attentes d'un plus grand nombre de parties prenantes. La divulgation volontaire et régulière serait donc un moyen pour elles de répondre aux attentes de leurs parties prenantes. La question de l'influence de la taille de l'entreprise sur la divulgation a été explorée par les chercheurs. Leurs conclusions fournissent des informations sur la façon dont la taille impacte l'étendue et la nature des informations relatives à la cybersécurité. Des études révèlent que les grandes entreprises sont plus disposées à divulguer de façon discrétionnaire les risques liés à la cybersécurité. Cette divulgation poussée des grandes entreprises repose sur un certain nombre de raisons.

D'une part, il faut noter que les grandes entreprises disposent généralement de plus de ressources aussi bien financières qu'humaines. De cette manière, elles ont la capacité de non seulement détecter, identifier et signaler les violations (Higgs *et al.*, 2016), mais aussi de mettre en place des mesures efficaces de gestion des risques de cybersécurité et ainsi fournir des informations plus complètes à leurs parties prenantes (Chen *et al.*, 2023 ; D'Arcy *et al.*, 2022 ; Mazumder et Hossain, 2023 ; Radu et Smaili, 2022). En revanche, les petites entreprises, dont les ressources sont plus limitées, n'ont pas la possibilité de fournir des informations aussi détaillées que leurs homologues (Radu et Smaili, 2022).

D'autre part, il faut souligner que plus l'entreprise est grande, plus la pression des parties prenantes est accrue. En effet, les régulateurs, les investisseurs et le public réclament plus de transparence

vis-à-vis des risques de cybersécurité. Les entreprises se livrent alors à des pratiques de divulgation pour satisfaire ces attentes et ainsi préserver leur réputation et renforcer la confiance des investisseurs (D'Arcy *et al.*, 2022 ; Li *et al.*, 2018 ; Mazumder et Hossain, 2023 ; Radu et Smaili, 2022).

En outre, l'une des raisons réside aussi dans la complexité de leurs opérations. Les grandes entreprises disposent de systèmes automatisés pour la réalisation de leurs activités. Ce qui signifie qu'elles sont plus sujettes aux cyberattaques et plus vulnérables aux violations de données. Par conséquent, elles adoptent des pratiques de divulgation proactive pour montrer leur engagement dans la gestion des risques de cybersécurité (D'Arcy *et al.*, 2022).

Néanmoins, Gao *et al.* (2020) soulignent que les grandes sociétés ont tendance à employer une terminologie plus large pour définir les vulnérabilités liées à la cybersécurité comparativement à leurs homologues de plus petite taille. Ils postulent qu'au fur et à mesure que l'entreprise se développe, les informations qu'elle communique semblent de plus en plus complexes à appréhender. Ils suggèrent que ce phénomène peut être imputé à l'augmentation de la complexité de l'environnement mondial et à la quantité d'informations requérant une divulgation.

1.2.3.2 L'endettement

L'endettement fait référence à la part des fonds qu'une entreprise a empruntés pour financer ses activités. Les chercheurs à travers leurs études l'ont mentionné comme un déterminant de la divulgation dans le sens où les entreprises subiraient des pressions de la part de leurs créanciers qui demandent plus de transparence.

En effet, Singh (2025) et Smaili *et al* (2023) ont trouvé une influence positive de l'endettement sur la divulgation en soulignant que les entreprises avec un haut niveau d'endettement ont tendance à communiquer davantage des renseignements en matière de cybersécurité. Ils affirment que cela découle du désir de ces entreprises de diminuer les coûts d'agences et l'asymétrie d'information existant entre les parties concernées, en particulier les investisseurs et les prêteurs. Ainsi, en divulguant plus d'informations, elles favorisent la transparence et la confiance, ce qui peut réduire les inquiétudes des prêteurs face aux risques de cybersécurité. L'étude de Alodat *et al.* (2024)

indique également une relation positive et significative entre le niveau d'endettement et la divulgation d'informations sur la cybersécurité ; ce qui pourrait suggérer que les entreprises fortement endettées sont poussées à accroître leur transparence pour apaiser leurs parties prenantes et diminuer l'asymétrie de l'information.

Mazumder et Hossain (2023) construisent leur argumentation en proposant, d'une part, que, selon une logique visant à réduire l'asymétrie d'information, les banques avec un niveau d'endettement élevé soient plus enclines à divulguer des informations relatives à la cybersécurité, étant donné que les investisseurs et autres parties prenantes peuvent intensifier leurs exigences vis-à-vis d'elles. Par ailleurs, ils suggèrent que les banques fortement endettées pourraient, dans certaines situations, décider de restreindre la transparence pour éviter de susciter des commentaires défavorables sur leur important niveau d'endettement. Finalement, leurs résultats ne mettent pas en évidence de relations notable entre le niveau d'endettement et la mesure de la divulgation volontaire en matière de cybersécurité pour les banques commerciales cotées au Bangladesh pendant la période étudiée. Cette non-significativité pourrait résulter du fait que l'étude ait été réalisée en considérant uniquement les banques, et ce, dans un contexte différent de la majorité des autres études concernant la divulgation de cybersécurité.

1.2.3.3 La rentabilité

Concernant la rentabilité, les conclusions de certains auteurs sont divergentes. De fait, Radu et Smaili (2022) soutiennent que la rentabilité est positivement associée à la divulgation de la cybersécurité, indiquant que les entreprises financièrement solides ont plus de ressources pour investir dans la gestion des risques et la communication sur ceux-ci. D'Arcy *et al* (2022) en revanche, trouvent que la rentabilité n'a pas de relation significative systématique avec les divulgations de cybersécurité, ce qui laisse à penser que la performance financière n'influence pas directement les décisions de divulgation dans ce contexte. Aussi, Mazumder et Hossain (2023) affirment que, bien que la rentabilité ait une relation positive avec la divulgation de la cybersécurité, elle n'est pas significativement associée, ce qui signifie que les banques plus rentables ne divulguent pas nécessairement davantage. Les investigations de Singh (2025) indiquent qu'il n'existe pas de relation significative entre la rentabilité et le degré de divulgation volontaire des risques liés à la cybersécurité. Contrairement à leur prédiction initiale, une forte rentabilité ne

pousse pas nécessairement à plus de transparence. L'auteur attribue cette absence de relation au fait que, dans le contexte indien, les divulgations sont plus influencées par des dynamiques de concurrence et des attentes propres au secteur, plutôt que par les résultats financiers des sociétés.

En résumé, les résultats empiriques sur l'impact de la rentabilité sur la divulgation de cybersécurité restent contradictoires dans la littérature. Certaines études révèlent une relation positive, tandis que d'autres ne mettent pas en évidence d'associations significatives. Ces contradictions pourraient s'expliquer par des facteurs institutionnels, temporels ou encore par la variabilité des indicateurs utilisés pour évaluer la divulgation de cybersécurité.

1.2.3.4 Le secteur d'activité

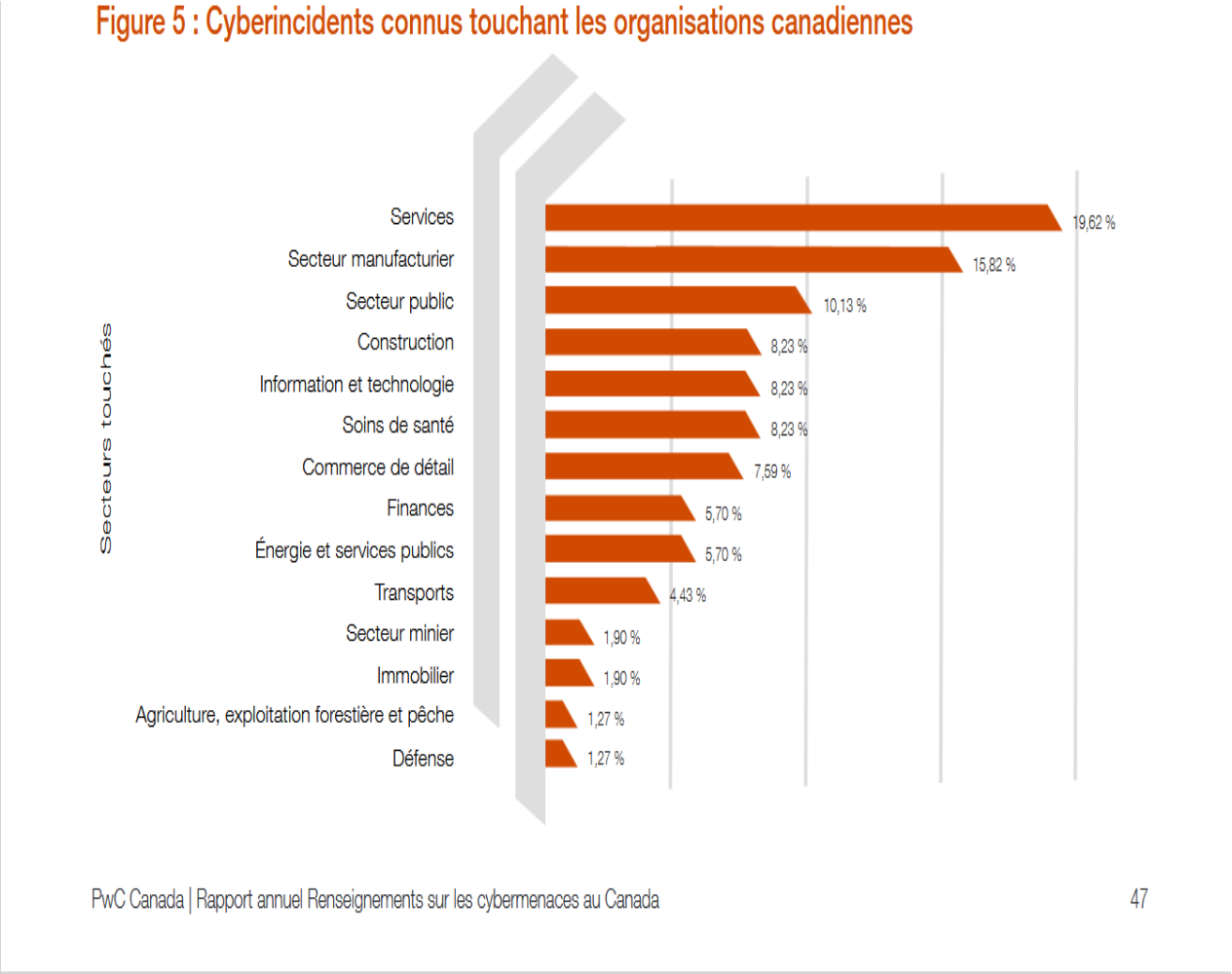
De façon générale, il faut noter que certains secteurs d'activité sont plus sensibles aux risques de cybersécurité que d'autres. À titre d'illustration, l'entreprise PwC Canada[7] a publié un rapport intitulé « Rapport annuel Renseignements sur les cybermenaces au Canada » dans lequel elle recense les différents secteurs qui ont été victime de cyberattaques au Canada en 2022. Ainsi, elle énumère dix principaux secteurs touchés au Canada, à savoir (voir la figure 1.1) :

- Services : 20 %
- Secteur manufacturier : 16 %
- Secteur public : 10 %
- Construction : 8 %
- Information et technologie : 8 %
- Soins de santé : 8 %
- Commerce de détail : 8 %
- Finances : 6 %

[7] https://www.pwc.com/ca/fr/services/consulting/cybersecurity-privacy/cyber-threat-intelligence/year-in-review.html#footnote consulté le 2025-03-01

- Énergie et services publics : 6 %
- Transports : 4 %

Figure 1.1 Secteurs d'activité des sociétés canadiennes les plus vulnérables aux cyberincidents



Source : (PwC, 2023), Page 47.

Étant donné qu'il existe des secteurs d'activité plus sensibles aux cyberincidents, il serait possible que les entreprises appartenant à ces secteurs communiquent davantage sur leur cybersécurité pour montrer leur engagement en ce qui concerne la gestion des risques de cybersécurité. Par exemple, l'étude de Smaili et al (2023) a porté sur un échantillon de 60 des plus grandes entreprises cotées à la Bourse de Toronto (S&P/TSX 60), qui provenaient de divers secteurs. Les secteurs les plus

représentés étaient l'énergie (18,33 %), les services financiers (16,67 %), les matériaux (13,33 %), la technologie de l'information (8,33 %) et les télécommunications (6,67 %). Les auteurs suggèrent que les sociétés opérant dans des secteurs jugés « sensibles au cyber-risque » (banques, assurances, technologies de l'information, communications et commerce en ligne) ont tendance à être plus transparentes concernant leurs pratiques de cybersécurité, répondant ainsi à une demande croissante de la part des parties prenantes. Cependant, le secteur de la santé (3,33 %) est le moins présent dans l'échantillon, ce qui indique une représentation réduite dans ce type particulier de divulgation. Ils concluent que la répartition par secteur met en évidence l'importance stratégique de la cybersécurité, particulièrement pour les industries les plus vulnérables aux menaces numériques et à la régulation.

La revue de littérature présentée dans ce chapitre a permis de mettre en lumière le cadre réglementaire régissant la divulgation en matière de cybersécurité ainsi que les pratiques de divulgation volontaire adoptées par les entreprises. Elle souligne également plusieurs facteurs susceptibles d'influencer l'étendue de cette divulgation, notamment la violation des données, les nouvelles directives de la SEC, les caractéristiques du conseil d'administration et les facteurs organisationnels (taille de l'entreprise, endettement, rentabilité, secteur d'activité). Cependant, les conclusions des auteurs quant à l'influence de certains déterminants de la divulgation de cybersécurité ne sont pas unanimes. Certaines études mettent en évidence des relations positives entre ces facteurs et la divulgation de cybersécurité, tandis que d'autres ne trouvent pas d'associations significatives ou obtiennent des résultats divergents selon les contextes étudiés. Ces divergences suggèrent que les déterminants de la divulgation de cybersécurité présentent toujours des parts d'ombre. Ainsi, cette recherche vise à s'inscrire dans la littérature existante en analysant les facteurs influençant la divulgation en matière de cybersécurité par les sociétés canadiennes cotées en bourse.

CHAPITRE 2
CADRE THÉORIQUE

Ce chapitre met en lumière les théories mobilisées pour analyser les facteurs qui influencent la divulgation de cybersécurité. De plus, il sert de base pour l'élaboration des hypothèses de recherche tout en soulignant les variables clés issues de la littérature et les relations attendues entre elles.

Avec les cyberattaques qui se multiplient à cause de l'évolution de l'environnement numérique, la cybersécurité est devenue un enjeu majeur pour les acteurs du tissu économique, entre autres : les entreprises, les parties prenantes et les régulateurs (SEC, ACVM). Le défi majeur est de réagir face à ces risques de cybersécurité. Par conséquent, les entreprises adoptent des pratiques de divulgation de cybersécurité réactives pour se conformer aux réglementations et proactives pour montrer leur engagement et renforcer la confiance des parties prenantes.

Toutefois, toutes les sociétés ne divulguent pas leurs stratégies de cybersécurité de façon identique. La différence entre elles peut résulter de certains facteurs incluant la fonction du conseil d'administration en tant que ressource interne et comme émetteur de signaux vers l'extérieur. Pour analyser les déterminants de la divulgation en matière de cybersécurité par les sociétés canadiennes cotées, ce mémoire se base sur deux approches théoriques : la théorie des ressources (RBV) et la théorie du signal.

2.1 La théorie des ressources

2.1.1 Les fondements de la théorie des ressources

La théorie des ressources ou RBV a été développée principalement par Jay Barney (1991) et s'appuie sur des travaux antérieurs de chercheurs comme Penrose (1958), Porter (1981), Wernerfelt (1984). Dans son article intitulé « *Firm Resources and Sustained Competitive Advantage* » (Barney, 1991), l'auteur a pour objectif de décrire les conditions environnementales qui favorisent les niveaux élevés de performance de l'entreprise. Pour ce faire, il considère deux hypothèses énoncées par ses homologues. La première suggère que les entreprises appartenant à un même secteur d'activité disposent de ressources homogènes et adoptent des stratégies similaires. Ce qui signifie que les entreprises sont identiques à l'intérieur d'une même industrie en termes de ressources et de

stratégies. La seconde suppose que, même s'il arrivait que les ressources ou stratégies diffèrent d'une entreprise à une autre, cette hétérogénéité ne sera pas durable, car les ressources sont mobiles, c'est-à-dire facilement transférables.

Cependant, Barney remet en question les hypothèses de départ émises par ses pairs en soutenant que celles-ci se situent dans un environnement majoritairement externe et par conséquent, le lien entre les caractéristiques internes et la performance d'une entreprise ne peut pas se baser sur ces mêmes hypothèses. Ainsi, il avance ses propres hypothèses. D'une part, il soutient que les ressources stratégiques des entreprises évoluant dans un même secteur peuvent être hétérogènes, c'est-à-dire différentes d'une entreprise à une autre. D'autre part, il suggère que l'hétérogénéité des ressources peut être durable, car il est difficile de transférer les ressources stratégiques. Il faut souligner que les deux hypothèses de Barney sont complètement opposées à celles de ses prédécesseurs.

De toutes ces hypothèses, il faut retenir qu'il y a un certain nombre de concepts qu'il convient de définir pour bien cerner la théorie des ressources.

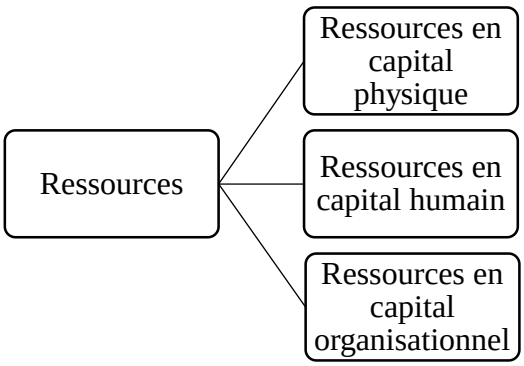
2.1.2 Définition des concepts de la RBV

Les concepts indispensables dont il convient de cerner le sens pour comprendre la théorie sont : ressource, avantage concurrentiel, avantage concurrentiel durable, hétérogénéité et mobilité. Les définitions retenues sont celles de Barney (1991).

- Ressources

Il s'agit de tous les actifs, capacités, processus organisationnel, attributs, informations, connaissances, etc., contrôlés par l'entreprise et qui lui permettent de concevoir et de mettre en œuvre des stratégies qui améliorent son efficience et son efficacité. L'auteur classe les ressources en trois catégories différentes : ressources physiques, les ressources humaines et les ressources organisationnelles. (Voir la figure 1.2)

Figure 2.1 Les catégories de ressources selon Jay Barney (1991)



Les ressources physiques comprennent toutes les immobilisations corporelles de la société : la technologie, les équipements et installations, la localisation géographique et l'accès aux matières premières.

Les ressources humaines englobent le leadership, la formation (les qualifications spécialisées), l'expérience, le jugement, et la perspicacité des différents cadres et employés d'une entreprise.

Les ressources organisationnelles incluent la structure formelle de l'entreprise, ses éléments de planification et de contrôle ainsi que des éléments informels, tels que les relations interpersonnelles et sa réputation (Booto Ekionea *et al.*, 2011).

- Avantage concurrentiel et avantage concurrentiel durable

Barney parle d'avantage concurrentiel lorsque l'entreprise met en œuvre une stratégie de création de valeur qui n'est pas simultanément mise en œuvre par des concurrents actuels ou potentiels. Dans le cas où les autres entreprises ne sont pas en mesure de reproduire les avantages de cette nouvelle stratégie, l'avantage concurrentiel devient un avantage concurrentiel durable. L'auteur souligne que la durabilité de l'avantage concurrentiel n'est pas une période calendaire, mais plutôt réside dans l'incapacité des concurrents actuels ou potentiels de copier cette stratégie.

- Hétérogénéité

Dans la première hypothèse de Barney, l'hétérogénéité des ressources signifie que les ressources stratégiques ne sont pas uniformément réparties entre les entreprises d'un même secteur.

- Immobilité

Dans la seconde hypothèse, l'immobilité signifie que les ressources ne peuvent pas être facilement achetées, transférées ou imitées par les concurrents.

2.1.3 Critères d'avantage concurrentiel d'une ressource : le cadre VRIN

Jay Barney estime que, pour qu'une ressource présente un avantage concurrentiel durable, elle doit disposer de quatre attributs distincts. Ainsi, les quatre indicateurs de l'hétérogénéité et de l'immobilité des ressources, selon l'auteur, se résument au cadre VRIN.

- Valuables (précieuse)
- Rare
- Imparfaitement inimitable
- Non substituable

En effet, selon l'auteur, une ressource est précieuse lorsqu'elle permet à l'entreprise de concevoir ou de mettre en œuvre des stratégies qui améliorent son efficacité et son efficience. En d'autres termes, les ressources de l'entreprise ne peuvent être source d'avantage concurrentiel que lorsqu'elles sont précieuses.

En outre, en ce qui concerne la rareté, une entreprise bénéficie d'un avantage concurrentiel soutenu lorsqu'elle met en œuvre une stratégie de création de valeur qui n'est pas mise en œuvre simultanément par un grand nombre d'autres entreprises. Cela signifie que si les ressources précieuses d'une entreprise sont absolument « uniques » parmi un ensemble d'entreprises concurrentes, elles génèreront un avantage concurrentiel.

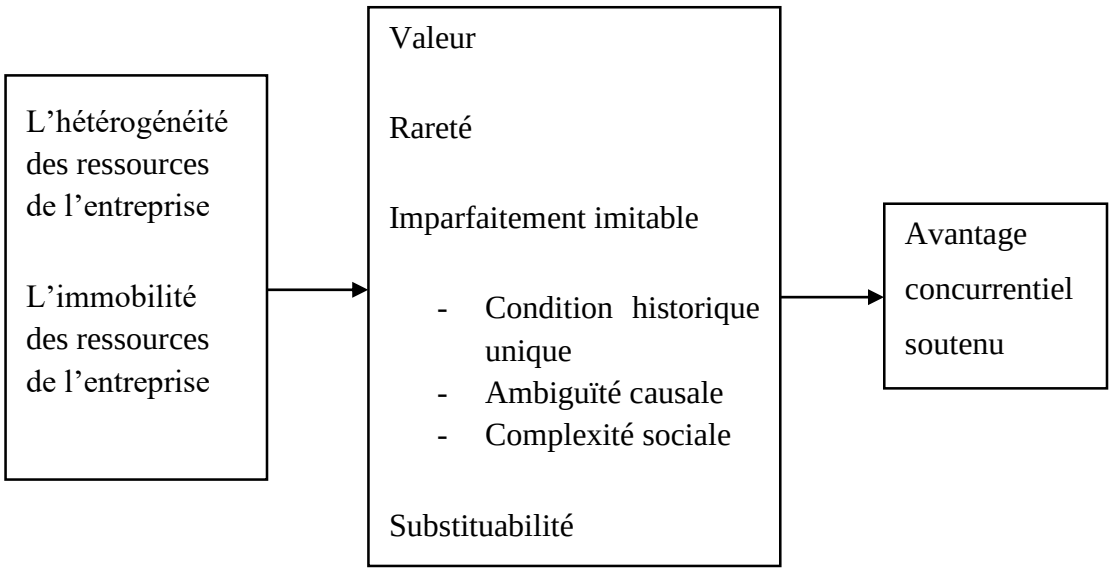
Toutefois, l'auteur souligne que pour être source d'avantage concurrentiel durable, les ressources précieuses et rares doivent être parfaitement inimitables. Pour cela, elles doivent respecter la triple condition suivante :

- La capacité d'une entreprise à obtenir une ressource dépend de sa condition historique ;
- Le lien entre les ressources possédées par une entreprise et l'avantage concurrentiel durable est causalement ambigu ;
- La ressource générant l'avantage d'une entreprise est socialement complexe.

Enfin, pour ce qui est de la substituabilité, Barney déclare qu'il ne doit pas avoir de ressources précieuses stratégiquement équivalentes qui ne sont pas elles-mêmes rares ou inimitables. De ce fait, la substituabilité peut prendre deux formes. Premièrement, bien qu'il soit impossible pour une entreprise d'imiter exactement les ressources d'une autre entreprise, elle peut les remplacer par une ressource similaire qui lui permet de concevoir et de mettre en œuvre les mêmes stratégies. Deuxièmement, il est possible que des ressources d'entreprises très différentes soient également des substituts stratégiques. Autrement dit, si suffisamment d'entreprises disposent de ces précieuses ressources de remplacement (c'est-à-dire qu'elles ne sont pas rares) ou si suffisamment d'entreprises peuvent les acquérir (c'est-à-dire qu'elles sont imitables) alors aucune de ces entreprises (y compris celles dont les ressources sont substituées) ne peut s'attendre à obtenir un avantage concurrentiel.

En définitive, la figure ci-dessous résume la relation entre l'hétérogénéité des ressources et l'immobilité, la valeur, la rareté, l'inimitabilité et la substituabilité.

Figure 2.2 Relation entre l'hétérogénéité et l'immobilité des ressources et l'avantage concurrentiel soutenu (Barney, 1991)



Source : Barney (1991, p. 112)

En somme, selon Barney, pour qu'une ressource présente un avantage concurrentiel, elle doit respecter toutes ces conditions.

2.1.4 Application de la théorie des ressources à la divulgation en matière de cybersécurité

La SEC, dans ses directives, recommande que les sociétés divulguent sur leur conseil d'administration en ce qui concerne leur rôle de surveillance des risques de cybersécurité. De ce fait, les entreprises prennent le soin de disposer de conseils qui remplissent efficacement ce rôle. Il existe également plusieurs études qui ont prouvé empiriquement que les conseils d'administration à travers leurs caractéristiques, notamment la taille, la diversité de genre, l'indépendance (Alodat *et al.*, 2024 ; Kurnia et Ardianto, 2024 ; Mazumder et Hossain, 2023 ; Radu et Smaili, 2022), l'expertise financière (Smaili *et al.*, 2023), l'expertise en TI, la présence de comité responsable de la cybersécurité (Héroux et Fortin, 2024) peuvent significativement influencer la divulgation des entreprises.

En revenant à la RBV, dans le cas de la divulgation de cybersécurité, le conseil d'administration pourrait être considéré comme une ressource à caractère humain. En se basant sur les explications

de Jay Barney, un conseil d'administration correctement constitué peut être présumé comme présentant un avantage concurrentiel dans la mesure où elle favorise une meilleure divulgation tant en quantité qu'en qualité.

2.1.4.1 Le conseil d'administration comme ressource stratégique et avantage concurrentiel

Étant donné que la littérature a démontré que le conseil à travers sa composition influence la divulgation de cybersécurité, alors il peut être considéré comme une ressource stratégique de l'entreprise qui lui procure un avantage concurrentiel. Il faut rappeler que, selon Barney (1991) pour qu'une ressource soit stratégique, elle doit être précieuse, rare, parfaitement inimitable et non substituable. Dans cette perspective, le conseil est une ressource stratégique, car :

- Il est précieux : avec un conseil large, l'entreprise dispose de plus d'administrateurs qui possèdent une expertise (financière, IT, cybersécurité, etc.).
- Il est rare : puisque les divulgations sur les risques de cybersécurité varient d'une entreprise à l'autre, il est évident que leurs conseils d'administration ne sont pas composés de la même manière. Cela dit, chaque conseil d'administration est unique du point de vue de la variété de ressources que les administrateurs lui apportent (Madhani, 2017).
- Il est inimitable : Madhani (2017) affirme que « les caractéristiques d'un conseil d'administration, telles que les connaissances et l'expérience de ses membres, sont beaucoup plus difficiles à imiter pour les concurrents que d'autres aspects de la composition du conseil, telles que la taille ou le ratio membres exécutifs/membres externes du conseil ».
- Il est non substituable : étant donné que le rôle de surveillance des risques de cybersécurité n'incombe qu'au conseil d'administration d'après les directives de la SEC, pour se conformer, les entreprises doivent absolument l'intégrer dans leurs pratiques de gestion de risques de cybersécurité.

En ce qui concerne l'hétérogénéité, Madhani (2017) remarque que la diversité d'expériences, de compétences et de connaissances des membres du conseil suggère que les ressources d'un conseil d'administration sont réparties de manière hétérogène entre les entreprises.

Dans la perspective des points énoncés, il est légitime de considérer le conseil d'administration comme ressource stratégique procurant un avantage concurrentiel.

2.1.4.2 Caractéristiques du conseil d'administration du point de vue de la RBV

Il existe des recherches qui sont basées sur la théorie des ressources afin d'explorer les tendances des caractéristiques du conseil d'administration. Parmi elles, on retrouve l'article de Krause *et al.* (2016) où les auteurs cherchent à explorer la perception des présidents du conseil d'administration comme ressources par leurs conseils respectifs en utilisant la théorie des ressources. Ainsi, il étudie la relation entre l'indépendance du président du conseil et l'effet du capital social sur la perception des ressources. L'étude a été réalisée sur un échantillon de 500 entreprises composant l'indice SP500 sur une période de 2 ans. Avec l'approche de la théorie des ressources, les auteurs postulent que les présidents du conseil peuvent être considérés comme ressources uniques pour l'entreprise en raison de leur capital humain et social. Ils indiquent que le capital humain se compose des compétences, des connaissances et l'expérience des présidents de conseil ; qui sont des atouts précieux. Ils désignent par capital social les réseaux de relations du président qui peuvent également être considérés comme ressources importantes. Leurs résultats suggèrent que le capital humain des présidents augmente la probabilité qu'un conseil les considère comme ressource précieuse. Par conséquent, conforté par les conclusions de Krause *et al.* (2016), ce mémoire peut soutenir que le conseil d'administration, à travers un président qui possède un capital humain, une expérience technique ou en cybersécurité, par exemple, peut être considéré comme une ressource.

Une autre étude, celle de Madhani (2017), en revanche, passe en revue les théories de la gouvernance d'entreprise afin de cerner les fonctions de la composition du conseil d'administration liées à la performance de l'entreprise. L'auteur avance que, du fait de la complexité des rôles des conseils, il a eu recours à de multiples théories pour atteindre son objectif de recherche. Parmi les théories abordées dans l'article se trouve celle des ressources. Il défend à cet effet que les membres du conseil d'administration lorsqu'ils sont activement impliqués dans la prise de décision stratégique soient considérés comme des ressources précieuses apportant des avantages concurrentiels grâce à leur connaissance transversale et leur expertise unique. Il soutient que « contrairement à la théorie de l'agence, qui met l'accent sur la gestion des objectifs conflictuels entre les dirigeants et les actionnaires au sein de l'entreprise, la RBV souligne le rôle que les administrateurs peuvent jouer en apportant des ressources uniques à l'entreprise » (Madhani, 2017).

Dans le contexte malaisien, Ismail *et al.* (2022) utilisent la théorie des ressources en tant que base théorique pour investiguer l'impact des capacités du conseil d'administration, en particulier leur taille, leur indépendance et leur diversité de genre sur la performance financière de 100 grandes sociétés cotées en bourse, de 2014 à 2018. Pour ce faire, les auteurs considèrent les capacités des administrateurs comme ressources cruciales pour la performance financière de l'entreprise. Les résultats de leur analyse de régression indiquent un effet significatif de la taille et de la diversité de genre sur la performance financière. En revanche, il n'a été prouvé aucun impact de l'indépendance du CA.

Toutefois, il faut remarquer que ces trois études énoncées précédemment ne traitent pas exactement de la divulgation de cybersécurité, mais plutôt de l'utilisation de la théorie des ressources en tant que base théorique pour étudier les caractéristiques du conseil d'administration comme ressource stratégique des entreprises. En réalité, dans la littérature, il n'existe pas beaucoup d'études menées sur la divulgation en matière de cybersécurité et traitant des caractéristiques du conseil. C'est pour cette raison que Sari *et al.* (2024) dans leur revue systématique portant sur les déterminants de la divulgation en matière de cybersécurité, n'ont identifié qu'une seule étude ayant utilisé cette théorie, notamment celle de Mazumder et Hossain (2023). En effet, l'article vise à mesurer l'étendue de la divulgation volontaire de cybersécurité dans les banques commerciales cotées au Bangladesh tout en examinant l'association entre la composition du conseil d'administration (taille, indépendance, diversité de genre) et cette divulgation. Afin d'atteindre leurs objectifs de recherche, ils ont adopté une triangulation de la théorie de l'agence et les perspectives de la théorie des ressources. Ils suggèrent que selon la RBV, un conseil d'administration avec une composition diversifiée apporte des ressources intellectuelles qui encouragent les pratiques de divulgation volontaires, telles que la divulgation de cybersécurité.

Tout en rappelant que l'objectif de cette étude est d'investiguer les déterminants de la divulgation en matière de cybersécurité par les entreprises canadiennes cotées, la théorie des ressources a été mobilisée pour servir de base dans la dérivation des hypothèses. Étant donné qu'il n'existe pas énormément de recherches à notre connaissance à cet effet, réalisé dans le contexte canadien, il serait important de contribuer théoriquement en complétant la littérature à ce propos.

2.2 La théorie du signal

2.2.1 Les fondements de la théorie du signal

La théorie des signaux a été développée par Michael Spence dans son essai intitulé « Job Market Signaling » (Spence, 1973). Dans ses travaux, Spence modélise le concept de signalisation sur le marché du travail où les candidats envoient des signaux pour révéler leur productivité potentielle aux employeurs. L'auteur tente de définir le concept de signalisation comme un partage d'informations entre les candidats et les employeurs à travers des signaux, comme le niveau d'éducation. Il faut comprendre ainsi qu'il existerait une asymétrie d'informations entre les potentiels candidats à un poste et leur employeur. Connelly *et al.* (2011) affirment à cet effet que « les travaux de Spence ont montré comment un candidat à l'emploi peut adopter un comportement visant à réduire l'asymétrie d'information qui entrave la capacité de sélection des employeurs potentiels ».

Par ailleurs, l'auteur postule que les candidats peuvent manipuler des signaux, tels que l'éducation, pour montrer leur productivité. De plus, il souligne que les coûts de signalisation en termes de temps et d'argent jouent un rôle important dans le choix des signaux par les individus. À titre d'exemple Connelly *et al.* (2011) expliquent que « Spence illustre comment les candidats qualifiés se distinguent des candidats de faible qualification grâce au signal coûteux d'une formation supérieure rigoureuse ».

En outre, Spence (1973) suggère que les caractéristiques observables et immuables, comme le sexe ou la race peuvent avoir un impact informationnel.

2.2.2 Définition des concepts de la théorie du signal

La théorie du signal fait appel à un certain nombre de concepts qu'il convient de comprendre. De ce fait les travaux de Connelly *et al.* (2011) sont une référence pour cerner les implications de cette théorie. En effet, l'article passe en revue la théorie des signaux, qui explique comment les parties possédant l'information communiquent pour réduire l'asymétrie. Il synthétise les concepts clés et les applications de la théorie dans diverses disciplines de gestion et souligne l'importance de comprendre le rôle de l'asymétrie de l'information et l'efficacité des signaux dans différents contextes.

Les auteurs évoquent trois concepts principaux qui sont : le signaleur, le récepteur et le signal. D'abord, les signaleurs sont définis comme « des initiés (par exemple, des cadres ou des gestionnaires) qui obtiennent des informations sur un individu (par exemple, Spence, 1973), un produit (par exemple, Kirmani et Rao, 2000) ou une organisation (par exemple, Ross, 1977) qui ne sont pas disponibles pour les personnes extérieures » (Connelly *et al.,* 2011, p. 44). Les auteurs soulignent que les informations obtenues par les initiés sont parfois positives, parfois négatives, que des personnes extérieures pourraient trouver utiles.

Ensuite, Connelly *et al.* (2011) énoncent que, selon cette théorie, le signal fait référence aux informations privées positives et négatives que les signaleurs doivent décider de communiquer délibérément aux personnes extérieures. Cependant, les auteurs soulignent que les signaux communiqués doivent avoir une double caractéristique pour être considérés comme efficaces. D'une part il y a « l'observabilité » du signal, qui désigne la capacité des personnes extérieures à percevoir ce signal. Ainsi, si les actions menées par les initiés ne sont pas aisément visibles pour les observateurs externes, il devient difficile de s'en servir comme moyen de communication avec les récepteurs (Connelly *et al.*, 2011). D'autre part, on retrouve le « coût du signal », qui signifie que certains émetteurs sont plus aptes que d'autres à supporter les dépenses associées. À cet effet, les auteurs expliquent que si le coût du signal est trop bas, des entreprises moins qualifiées pourraient tenter de tricher, rendant le signal inutile. Alors, pour éviter cela, les signaux doivent être assez coûteux pour décourager les fraudeurs, tout en restant accessibles à ceux qui possèdent réellement la qualité qu'ils indiquent (Connelly *et al.*, 2011).

Enfin, « les récepteurs sont des personnes extérieures à l'organisation qui ne disposent pas d'informations sur elle, mais qui souhaiteraient les recevoir » (Connelly *et al.*, 2011, p. 45). Mais, selon les auteurs, il se trouve que, souvent, les signaleurs et les récepteurs n'ont pas toujours les mêmes intérêts ; ce qui peut entrainer des situations où un signaleur peut être tenté de tromper un récepteur pour en tirer un avantage.

En ramenant les concepts décrits plus haut dans le cadre de ce mémoire, les signaleurs sont les entreprises à travers leur conseil d'administration ; les récepteurs sont ses parties prenantes, notamment les investisseurs, les régulateurs, les clients, les fournisseurs, etc., et le signal est la divulgation d'information en matière de cybersécurité.

2.2.3 Application de la théorie du signal dans le cadre de la divulgation de cybersécurité

Dans les recherches réalisées sur la divulgation en matière de cybersécurité, nombre d'entre elles ont utilisé la théorie du signal comme cadre théorique de leurs études. Par exemple, dans l'une d'entre elles, les auteurs ont analysé les divulgations en matière de cybersécurité chez 48 banques canadiennes et américaines en utilisant la théorie du signal pour déterminer dans quelle mesure ces divulgations servent à montrer l'engagement des banques envers la gestion des risques de cybersécurité et à renforcer leur légitimité (Firoozi et Mohsni, 2023). Avec un cadre théorique fondé sur les théories des signaux et de légitimité, les auteurs prédisent une divulgation plus élevée en matière de cybersécurité, spécialement lors d'une violation de données, car les entreprises sont davantage incitées à signaler leurs engagements aux parties prenantes face à cette situation.

De même, dans le contexte indien, Singh (2025) fait intervenir plusieurs théories, notamment celle du signal, pour examiner les divulgations volontaires des risques de cybersécurité des entreprises indiennes cotées en bourse. S'appuyant sur les affirmations d'autres auteurs, il suggère que les entreprises indiennes cherchent à signaler leur qualité et leurs capacités en divulguant plus d'informations sur les risques de cybersécurité. Ainsi, se référant à Elshandidy et al (2013), les auteurs prédisent que les entreprises très rentables disposent de ressources supplémentaires à investir dans la gestion des cybermenaces, leur permettant ainsi de diffuser davantage d'informations ; ce qui n'est pas toujours le cas des petites entreprises.

La théorie du signal a été également interpellée dans les études faisant intervenir le conseil d'administration dans le cadre des divulgations en matière de cybersécurité. Parmi elles, l'étude de Smaili *et al* (2023) s'est appuyée sur la théorie du signal pour expliquer que les entreprises utilisent la divulgation de cybersécurité comme signal pour démontrer qu'elles gèrent de façon proactive les risques de cybersécurité. À cet effet, les auteurs suggèrent qu'un conseil d'administration, de par l'indépendance, l'expertise financière de ses membres est plus encline à communiquer sur la cybersécurité afin de rassurer les parties prenantes.

Higgs *et al.* (2016) dans leur recherche, suggèrent que la création d'un comité technologique au niveau du conseil d'administration sert de signal pour démontrer que l'entreprise prend au sérieux la gouvernance des risques technologiques, car ils estiment que le comité s'impliquerait activement

dans la surveillance des risques. Étant donné qu'un signal efficace est déterminé par son coût (Spence, 1973), les auteurs, par conséquent, soulignent que la mise en place d'un comité technologique au niveau du conseil est coûteuse dans la mesure où il impliquerait une charte, des réunions obligatoires, une rémunération supplémentaire et la communication d'informations dans les circulaires concernant ses activités. Leurs prédictions se sont avérées juste, car leurs résultats ont indiqué que les entreprises avec des comités technologiques sont plus susceptibles de signaler les violations de cybersécurité contrairement à celles qui n'en disposent pas.

Toujours dans le contexte de divulgation de cybersécurité par les conseils d'administration, Héroux et Fortin (2024) font intervenir la théorie du signal pour prouver que certaines caractéristiques du conseil, à savoir l'expertise en TI, la diversité de genre, l'indépendance, peuvent signaler une meilleure gouvernance en matière de cybersécurité. Leurs résultats apportent également les preuves que la présence d'un comité responsable de la cybersécurité au sein du conseil est un signal fort soulignant l'engagement de l'entreprise en termes de gestion des risques informatiques.

2.3 Rôle et complémentarité des cadres théoriques mobilisés

Deux cadres théoriques, soit la théorie des ressources et la théorie du signal, sont utilisés dans ce mémoire pour étudier la divulgation en matière de cybersécurité. Cependant, il est important de clarifier leur rôle respectif dans l'analyse pour mettre en évidence leur contribution.

D'une part, la théorie des ressources permet d'appréhender les caractéristiques internes de l'entreprise comme des ressources stratégiques pouvant affecter sa capacité à gérer et à encadrer les défis de la cybersécurité. En effet, certains aspects du conseil d'administration, tels que sa taille, son indépendance, sa diversité ou encore son expertise, peuvent être perçus comme des ressources internes renforçant la gouvernance, et, par extension, la tendance à communiquer sur des questions de cybersécurité.

D'autre part, la théorie du signal fournit un cadre d'analyse pour interpréter la divulgation comme un outil de communication dans des situations d'asymétrie d'information entre l'entreprise et ses parties prenantes. La divulgation proactive d'informations sur la cybersécurité peut être interprétée comme un signal envoyé au marché visant à réduire l'incertitude, à renforcer la crédibilité de l'entreprise et à influencer la perception des investisseurs.

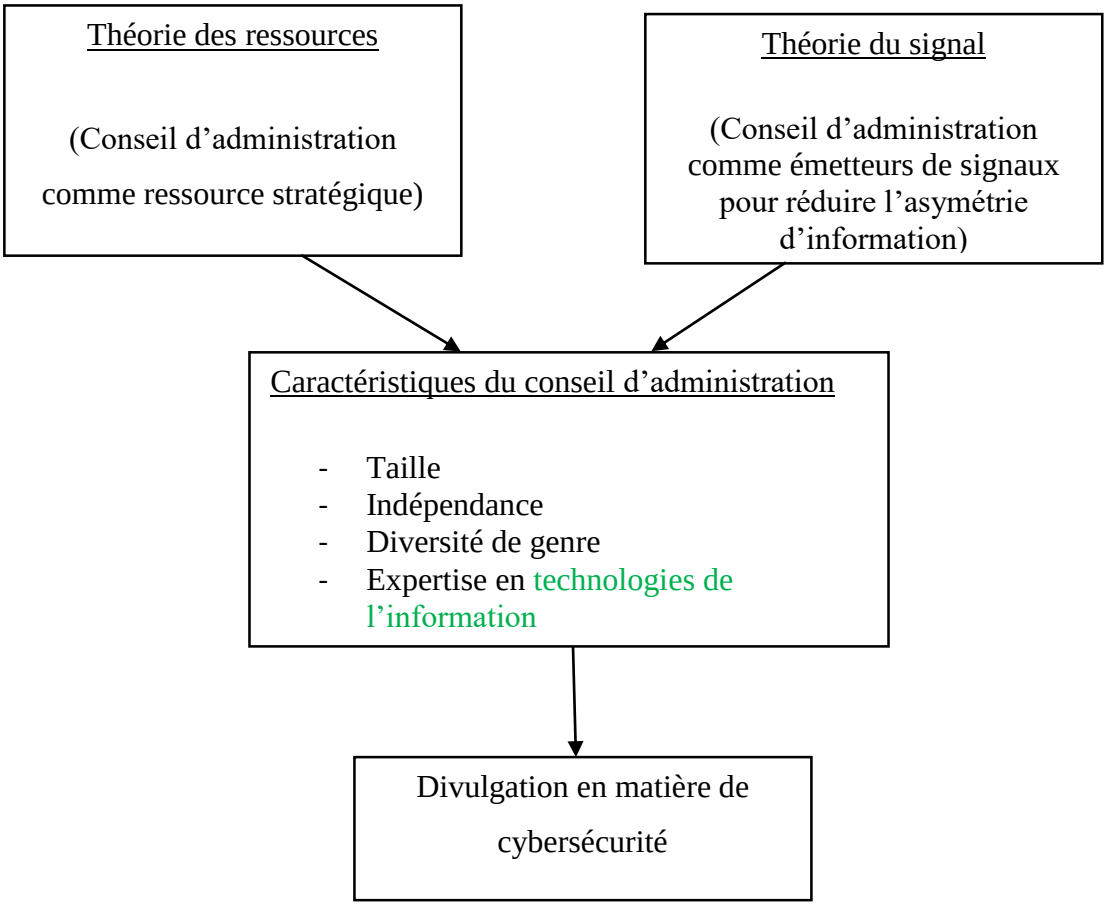
Ainsi, ces deux cadres ne poursuivent pas le même objectif analytique. La théorie des ressources sert principalement à expliquer les facteurs organisationnels qui peuvent influencer la divulgation, tandis que la théorie du signal permet d'en comprendre la dimension informative et tactique. Leur action combinée permet de lier les traits internes de l'entreprise à la portée externe de la divulgation.

Il est important de noter que l'étude s'engage dans une analyse empirique pour mettre en évidence des liens entre des caractéristiques organisationnelles spécifiques et la divulgation en matière de cybersécurité. Les cadres théoriques mobilisés servent ainsi à éclairer l'interprétation des résultats empiriques.

En somme, en prenant pour référence les travaux des auteurs mentionnés dans ce cadre théorique, cette étude retient l'application conjointe des théories des ressources et du signal pour analyser les déterminants de la divulgation en matière de cybersécurité par les entreprises canadiennes cotées. Dans la mesure où la SEC insiste sur le rôle de surveillance du conseil d'administration dans la gestion des risques de cybersécurité, cette recherche va s'articuler autour des caractéristiques du conseil comme déterminants de la divulgation de cybersécurité. D'une part, comme Mazumder et Hossain (2023), nous considérons le conseil d'administration de par sa taille, l'indépendance, la diversité de genre, l'expertise en technologies de l'information de ses membres comme une ressource stratégique qui favorise la divulgation proactive en matière de cybersécurité. De surcroît, soutenu par cette affirmation indiquant que « l'amélioration de la divulgation des informations sur la cybersécurité témoigne de la capacité du conseil d'administration à anticiper les cyberattaques et à protéger les intérêts des parties prenantes » (Smaili *et al.,* 2023), on note l'importance du conseil d'administration dans la gestion des risques de cybersécurité, par conséquent, la divulgation à cet effet. D'autre part, vu que l'essence de la théorie du signal réside dans le fait qu'une partie plus informée et détenant l'information la communique à l'autre sous forme de signal pour l'aider dans la prise de décision (Spence, 1973), nous soutenons l'idée qu'un conseil d'administration bien constitué pourrait réduire l'asymétrie d'information entre l'entreprise et ses parties prenantes (Smaili *et al.,* 2023). Cela dit, nous nous attendons à ce que les entreprises à travers l'indépendance, la diversité de genre et l'expertise en technologies de l'information des membres de leurs conseils d'administration soient plus transparentes vis-à-vis de leurs parties prenantes en divulguant davantage pour signaler leur engagement en termes de gestion des risques de cybersécurité (Héroux

et Fortin, 2024). Ainsi, à travers la figure suivante, nous schématisons le cadre théorique retenu pour cette étude.

Figure 2.3 Schéma du cadre théorique



Source : L'auteur

CHAPITRE 3
DÉVELOPPEMENT D'HYPOTHÈSES

Dans le contexte où les entreprises adoptent des pratiques de divulgation pour répondre aux attentes de leurs parties prenantes en matière de cybersécurité, le conseil d'administration à travers ses caractéristiques peut influencer positivement cette divulgation grâce à son rôle de surveillance. Dans ce chapitre, il est question de développer les hypothèses de recherche en prenant comme assertion de base les théories des ressources et du signal, tout en s'appuyant sur les données de la revue de littérature. Le but est de parvenir à identifier, pour un conseil d'administration type, les caractéristiques qui déterminent la divulgation en matière de cybersécurité par les entreprises canadiennes cotées.

3.1 Rappel des éléments théoriques pertinents pour le développement d'hypothèses

Cette étude mobilise conjointement la théorie des ressources et la théorie du signal afin d'analyser les facteurs qui influencent la divulgation en matière de cybersécurité par les entreprises. Étant donné que la SEC met particulièrement l'accent sur le rôle de supervision du conseil d'administration dans la gestion des cyberrisques, cette recherche choisit de se concentrer sur les caractéristiques du conseil comme déterminants de la divulgation.

D'une part, dans la lignée des travaux de Mazumder et Hossain (2023), nous considérons le conseil d'administration comme une ressource stratégique. Plus spécifiquement, ses caractéristiques, notamment la taille, l'indépendance, la diversité de genre et l'expertise en technologies de l'information de ses membres peuvent, selon nous, être perçues comme des ressources stratégiques incitant à une communication proactive en matière de cybersécurité. En effet, Smaili *et al* (2023) font remarquer que plus la divulgation est structurée et claire, plus elle reflète la capacité du conseil à anticiper les menaces numériques et à défendre les intérêts des différentes parties prenantes.

D'autre part, si l'on se réfère à la logique de la théorie du signal (Spence, 1973), qui repose sur la transmission d'informations crédibles d'un acteur mieux informé à un autre afin de réduire les incertitudes dans la prise de décision, cette étude soutient comme Smaili *et al.* (2023) qu'un conseil d'administration bien structuré pourrait contribuer à réduire l'asymétrie d'information entre

l’entreprise et ses parties prenantes. Ainsi, on peut s’attendre à ce que les entreprises dont les conseils d’administration se distinguent par une plus grande indépendance, une diversité de genre marqué et une solide expertise en technologies de l’information soient plus aptes à faire preuve de transparence envers leurs parties prenantes. En effet, soutenu par Héroux et Fortin (2024) ces caractéristiques pourraient les amener à divulguer davantage d’informations en matière de cybersécurité, dans le but de démontrer leur engagement et leur sérieux dans la gestion des risques liés aux cybermenaces.

En effet, la structure du conseil d’administration d’une entreprise joue un rôle crucial dans l’établissement des procédures de divulgation de cybersécurité. Cette étude formule donc quatre hypothèses en se basant sur les caractéristiques du conseil, telles que son indépendance, la diversité de genre, l’expertise en technologies de l’information et sa taille. Dans les prochaines sections, il sera question de présenter les relations présumées entre ces caractéristiques et la divulgation en matière de cybersécurité, tout en se référant aux résultats de diverses recherches.

3.2 Élaboration des hypothèses

3.2.1 L’indépendance du conseil d’administration

Étant donné que la théorie du signal mobilisée pour cette étude énonce l’idée de la réduction de l’asymétrie d’informations vis-à-vis des parties prenantes qui sont de plus en plus concernées par leur cybersécurité, la divulgation volontaire d’informations sur cette dernière est la stratégie adoptée par les entreprises. Il se trouve que l’indépendance du conseil d’administration a fait sujet de nombreuses réflexions, comme en témoignent plusieurs études qui ont prouvé son influence sur la divulgation volontaire. Par exemple, Lim *et al.* (2007) ont trouvé que plus les conseils d'administration disposent d'administrateurs indépendants, plus elles divulguent volontairement d'informations quantitatives et stratégiques tournées vers l'avenir. En effet, ils soutiennent que les administrateurs indépendants sont incités à divulguer volontairement des informations dans le but de protéger leur réputation et réduire les risques de litige et l'asymétrie de l'information. Par conséquent, il est légitime de s’attendre à ce que l’indépendance du conseil d’administration soit également un facteur déterminant de la divulgation en matière de cybersécurité.

En outre, il faut noter que les administrateurs indépendants sont en mesure de donner un jugement impartial et objectif sur les résolutions du conseil d'administration, ce qui peut renforcer la surveillance des procédures de cybersécurité. Les recherches ont démontré que des niveaux élevés d'indépendance au sein des conseils d'administration sont positivement associés à de meilleures pratiques de divulgation en matière de cybersécurité. À titre d'illustration, des études menées sur les entreprises financières indiennes ont conclu que la diversité d'indépendance du conseil améliore considérablement les niveaux de divulgation de cybersécurité (Shukla et Pandey, 2023). Dans l'article, la diversité d'indépendance fait référence à la variété et à l'équilibre des administrateurs indépendants au sein du conseil d'administration d'une entreprise. Les auteurs soutiennent que cette diversité est essentielle pour garantir une prise de décision impartiale et une gouvernance efficace.

Par ailleurs, il a été également soutenu que les conseils d'administration indépendants agissent comme « mécanisme de gouvernance et de surveillance » (Smaili *et al.*, 2023) et qu'ils favorisent la transparence et la bonne gouvernance (Alodat *et al.*, 2024). Ainsi, leurs conclusions indiquent une influence positive de l'indépendance sur la divulgation de cybersécurité. De plus, Héroux et Fortin (2024), tout en confirmant ces résultats, postulent que les administrateurs indépendants, grâce à la transversalité de leurs points de vue et de leurs compétences, sont susceptibles de favoriser une communication plus complète et transparente sur ces enjeux.

Du point de vue de la théorie des ressources, les administrateurs indépendants disposent davantage de ressources, comme une expertise pertinente, des connaissances actuelles, des réseaux professionnels et sociaux et une légitimité, qui influencent les comportements et la prise de décision des entreprises (Mazumder et Hossain, 2023)

L'influence positive du conseil d'administration sur la divulgation de cybersécurité peut être imputée à la compétence des administrateurs indépendants pour remettre en question les choix de gestion et s'assurer que les enjeux de cybersécurité sont pris en charge. Dans cette perspective, les administrateurs indépendants sont plus enclins à exiger une transparence et une responsabilité accrues en matière de cybersécurité, induisant inévitablement la génération de données plus exhaustives.

Soutenue par les arguments avancés dans les précédents paragraphes, cette recherche suppose que les administrateurs indépendants sont plus susceptibles de promouvoir la transparence pour répondre aux attentes des parties prenantes. Il s'agit là du fondement de la première hypothèse à savoir :

H1 *: L'indépendance du conseil d'administration est positivement associée au niveau de divulgation des informations en matière de cybersécurité.*

3.2.2 La diversité de genre au sein du conseil d'administration

Le niveau de divulgation d'informations en matière de cybersécurité a également été associé à la diversité de genre au sein du conseil d'administration. Des études montrent que les conseils d'administration qui présentent une diversité de genre sont plus disposés à adopter des mesures proactives en matière de cybersécurité et à communiquer des informations pertinentes aux parties prenantes, car les femmes directrices de par leurs natures intrinsèques sont plus sensibles aux risques et aux responsabilités sociales (Héroux et Fortin, 2024).

Selon une recherche portant sur les entreprises canadiennes, il a été mis en évidence que les conseils d'administration comprenant un nombre significatif d'au moins trois femmes affichent des niveaux de divulgation de cybersécurité supérieurs (Radu et Smaili, 2022). Par ailleurs, une recherche concernant les banques en Indonésie a démontré que la présence de femmes dans le conseil des commissaires a un impact positif sur cette divulgation, même si l'impact de la masse critique d'au moins trois femmes n'a pas été constaté (Kurnia et Ardianto, 2024).

Toutefois, certains auteurs n'ont pas pu conclure de l'impact positif de la présence de femmes au conseil d'administration sur la divulgation de cybersécurité. En effet, l'étude de Shukla et Pandey (2023) révèle que la diversité de genre n'a pas d'impact significatif sur la divulgation de cybersécurité. Ils estiment que le simple fait d'avoir des conseils d'administration plus diversifiés en termes de genre peut ne pas influencer directement la manière dont les entreprises divulguent les informations relatives à la cybersécurité. Pour leur part, Alodat *et al.* (2024) ont trouvé un effet positif, mais non significatif entre la diversité de genre au sein du conseil et l'étendue de la divulgation. Selon les auteurs, cette absence de significativité serait due à la prudence des

administratrices qui tendraient à limiter la communication de certaines informations sensibles sur cybersécurité, afin d'éviter que celles-ci ne tombent entre les mains des personnes malveillantes.

En revenant sur la théorie du signal, Spence (1973) suggère que des caractéristiques observables et immuables, telles que le genre, peuvent avoir une incidence sur la manière dont l'information est produite, traitée ou communiquée. Ainsi, il peut être légitime de considérer la diversité de genre comme facteur déterminant de la divulgation de cybersécurité ; dans la mesure où les femmes du conseil seraient plus favorables à divulguer davantage. Les travaux de Elnahass *et al.* (2024) ont apporté les preuves empiriques selon lesquelles, les administratrices sont plus aptes à partager des informations en rapport avec la cybersécurité et à fournir des détails bien plus précis que leurs collègues masculins ; d'où l'importance de la diversité de genre pour la transparence des entreprises concernant leurs pratiques en matière de cybersécurité.

La théorie basée sur les ressources, quant à elle, soutient que les administratrices apportent à leur conseil d'administration des ressources et des relations uniques et précieuses qui sont différentes et souvent meilleures que celles provenant de leurs homologues masculins (Mazumder et Hossain, 2023). Cela pourrait exercer une influence sur le niveau de divulgation.

Dans la lignée des travaux des chercheurs mentionnés ci-dessus, cette étude s'attend à ce que la présence de femmes au sein du conseil d'administration améliore la gouvernance et renforce simultanément la sensibilité à la transparence. C'est bien là, le soubassement de la seconde hypothèse qui s'énonce comme suit :

***H2** : La diversité de genre au sein du conseil d'administration est positivement associée au niveau de divulgation en matière de cybersécurité*

3.2.3 La taille du conseil d'administration

Pour ce qui est de l'influence de la taille du conseil d'administration sur la divulgation en matière de cybersécurité, les résultats des chercheurs restent encore mitigés. En effet, une recherche portant sur la relation entre la composition du conseil d'administration et les brèches de sécurité de l'information a démontré qu'un conseil d'administration plus conséquent pourrait accroître le risque

des violations de sécurité, en raison d'éventuelles difficultés dans la communication et la coordination (Wang et Hsu, 2010). En d'autres termes, les auteurs suggèrent qu'un conseil relativement grand du point de vue du nombre de ses membres peut avoir un impact négatif sur son efficacité dans la supervision de la gestion de la sécurité de l'information.

Certaines études, quant à elles, n'ont pas pu mettre en évidence de liens significatifs entre la taille du conseil et la divulgation (Mazumder et Hossain, 2023 ; Smaili *et al.*, 2023). Ils indiquent à cet effet que l'impact de la taille du conseil pourrait varier en fonction d'autres éléments, tels que l'indépendance et l'expertise spécifique à la cybersécurité chez la plupart des administrateurs.

Cependant, pour certains, la taille du conseil exerce une influence positive et significative sur la divulgation. C'est par exemple le cas de Alodat *et al.* (2024) qui, dans le contexte britannique, ont pu apporter les preuves de leur assertion. Ils affirment que les entreprises dont le conseil d'administration est plus grand fournissent davantage d'informations en matière de cybersécurité. De plus, les auteurs soutiennent que, selon la théorie de l'agence, ce résultat est confirmé par les conseils d'administration plus grands qui mettent en œuvre des mesures de contrôle efficaces pour réduire les risques.

En considérant la définition de la taille du conseil, qui n'est autre que le nombre d'administrateurs le constituant, un conseil de plus grande taille aura tendance à faciliter l'intégration d'administrateurs aux compétences variées, telle que des experts en cybersécurité ou en gestion des risques technologiques, ce qui peut renforcer la qualité et la profondeur des divulgations en matière de cybersécurité. De plus, en s'appuyant sur le cadre théorique de la RBV développée dans la revue de littérature, le caractère précieux du conseil peut être lié à sa taille dans la mesure où, avec un conseil plus large, l'entreprise dispose de plus d'administrateurs qui possèdent une expertise (financière, IT, cybersécurité, etc.) indispensable pour la gestion des risques de cybersécurité. Cette transversalité en relation directe avec la taille du conseil d'administration constitue la base de la formulation de la troisième hypothèse qui s'énonce comme suite :

***H3** : La taille du conseil d'administration est positivement associée au niveau de divulgation en matière de cybersécurité.*

3.2.4 L’expertise en technologies de l’information du conseil d’administration

L’expertise en technologies de l’information du conseil d’administration dans cette étude fait référence à un niveau élevé de connaissances et de compétences spécialement dans les domaines informatiques et de cybersécurité que possèdent les administrateurs. D’abord, les investigations de Hartmann et Carmenate (2021) ont remarqué que, malgré le fait que les enjeux de cybersécurité soient majeurs, de nombreuses études indiquent que les conseils d’administration manquent souvent d’expertise technologique. Par conséquent, les entreprises adoptent diverses approches, comme l’intégration d’experts en technologie dans le conseil, la création de comités IT dédiés, ou le transfert partiel des responsabilités vers le comité d’audit.

Par la suite, le rapport 2023 de Spencer Stuart[8] sur la gouvernance des conseils d'administration des 100 plus grandes entreprises canadiennes a relevé que les administrateurs indépendants nommés au conseil possédant une expérience de base dans le domaine des technologies (notamment en informatique, plateformes numériques, IA, cybersécurité, données et analyses) et une expérience pertinente en matière de transformation numérique étaient également plus demandés.

Enfin, Smaili *et al.* (2023) ayant exploré l’impact de l’expertise financière sur la divulgation de cybersécurité ont recommandé aux recherches futures d’étudier d’autres compétences et expertises importantes du conseil d’administration, telles que l’expertise en technologies de l’information (informatique), juridique ou éthique, car l’évaluation et la gestion des cyberrisques exigent la contribution de plusieurs disciplines.

La littérature montre que le niveau de divulgation en matière de cybersécurité est également influencé par la présence de spécialistes en technologie au conseil d’administration, un aspect non négligeable. Les spécialistes techniques ont la capacité de fournir une expertise et des compétences spécifiques qui aident le conseil d'administration à appréhender et à gérer plus efficacement les risques liés à la cybersécurité. À titre d’illustration, une recherche concernant les entreprises financières en Inde a démontré que l'inclusion d'un expert en informatique au sein du conseil d'administration entrainait une augmentation notable des niveaux de divulgation de cybersécurité

[8] https://www.spencerstuart.com/research-and-insight/canada-board-index consulté le 2025-04-12

(Shukla et Pandey, 2023). Par ailleurs, des études réalisées sur les entreprises au sein de la région MENA[9] ont mis en évidence l'importance d'une expertise en informatique pour optimiser les méthodes et les divulgations relative à la cybersécurité (Al-Sartawi, 2020). Ils soutiennent que cette expertise leur permet de superviser et de remettre en question efficacement les actions des responsables informatiques, ce qui permet d'améliorer les pratiques de cybersécurité et la transparence des divulgations. Dans le contexte canadien, Héroux et Fortin (2024) ont démontré que l'expertise informatique des membres du conseil est positivement associée à l'étendue de la divulgation de la cybersécurité. Les auteurs suggèrent que « ces connaissances et cette expérience « spécialisées » liées à l'informatique constituent un atout lorsqu'il s'agit de décider quelles informations divulguer et d'utiliser les termes appropriés pour le faire ».

Pour continuer, d'autres recherches sur l'impact de l'expertise en informatique des comités d'audit sur les violations de données soutiennent aussi le rôle que joue cette compétence dans la divulgation de cybersécurité. Ainsi, les travaux de Chen *et al.* (2022) ont démontré que les comités d'audit ayant une compétence en informatique sont plus performants pour surveiller et gérer les risques de cybersécurité, contribuant ainsi à la diminution des violations de données. Dans la même lignée que ces résultats, Héroux et Fortin (2024) ont confirmée plus tard que la présence d'un comité responsable de la cybersécurité au sein du conseil est positivement associée à l'étendue de la divulgation de la cybersécurité. Les auteurs suggèrent que ce comité signale que le conseil prend au sérieux les questions de cybersécurité et est prêt à s'impliquer dans la divulgation.

À la lumière de tous ces arguments, cette recherche retient que l'expertise en technologies de l'information des administrateurs est une ressource précieuse du point de vue de la théorie des ressources, car elle peut présenter un avantage concurrentiel. Cela dit, les entreprises disposant d'admirateurs spécialistes en informatique et cybersécurité auront tendance à divulguer davantage que celles qui n'en disposent pas. Ainsi, la supposition que les administrateurs dotés de compétences techniques en cybersécurité ou en informatique comprennent mieux les enjeux et

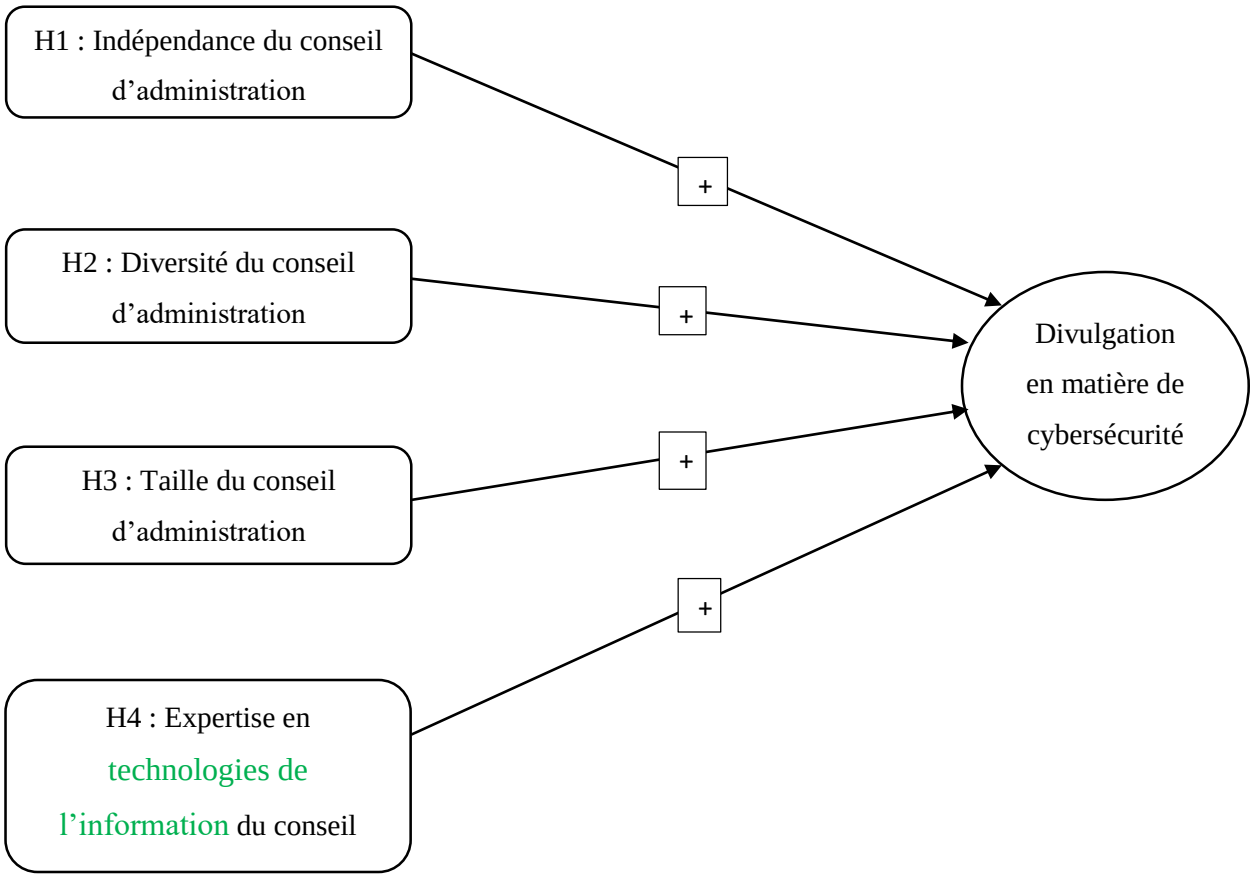
[9] **Middle East and Northern Africa** (MENA) désigne les pays qui bordent le Sud de la Méditerranée ainsi que la péninsule arabique (https://www.eurofiscalis.com/lexiques/mena/)

favorisent une communication plus poussée, claire et précise constitue le socle de la quatrième hypothèse qui s'énonce de la façon suivante :

H4 : La présence d'administrateurs possédant une expertise en technologies de l'information est positivement associée au niveau de divulgation des informations en matière de cybersécurité.

Pour illustrer les hypothèses émises afin d'analyser les déterminants de la divulgation en matière de cybersécurité par les entreprises, nous avons élaborer un schéma conceptuel montrant la relation attendue entre les caractéristiques du conseil d'administration, spécifiquement l'indépendance, la diversité de genre, la taille, l'expertise en technologies de l'information et le niveau de divulgation en matière de cybersécurité. (Voir figure 2.1)

Figure 3.1 Schéma conceptuel du modèle de recherche



Source : L'auteur

CHAPITRE 4
MÉTHODOLOGIE DE RECHERCHE

Ce chapitre détaille la démarche adoptée pour analyser l'impact des caractéristiques du conseil d'administration sur la divulgation en matière de cybersécurité par les entreprises. Il décrit à cet effet le type de recherche, l'échantillon, la méthode de collecte de données, les variables de l'étude ainsi que les méthodes d'analyse statistique utilisées.

4.1 Motivation du choix de la méthodologie

Ce mémoire utilise une méthode mixte pour explorer les caractéristiques du conseil d'administration en tant que déterminants de la divulgation en matière de cybersécurité par les entreprises.

Dans un premier temps, une approche qualitative est mobilisée à travers une analyse de contenu automatisée réalisée à partir du logiciel Nvivo. Cette démarche permet de mesurer et de quantifier la divulgation d'informations liées à la cybersécurité dans les rapports annuels. Les résultats issus de cette analyse constituent la base pour l'étape suivante.

Dans un deuxième temps, la méthode quantitative soutenue par une analyse de régression est retenue. Cette dernière est utilisée dans les études de corrélation qui examinent les liens entre une variable explicative et une variable expliquée (Statistiques pour la gestion, 2017). Ainsi, pour analyser l'impact des caractéristiques du conseil d'administration sur la divulgation en matière de cybersécurité, cette recherche développe un modèle de régression.

Les détails relatifs aux deux méthodes pour parvenir à l'analyse sont détaillés dans la suite du chapitre.

4.2 Sélection de l'échantillon

L'étude portant sur l'analyse des déterminants de la divulgation en matière de cybersécurité est menée sur une population d'entreprises canadiennes cotées en bourse. L'échantillon est donc composé des 60 sociétés cotées à la Bourse de Toronto (TSX) qui figurent sur l'indice S&P/TSX 60.

Cet indice représente la composante canadienne de l'indice international S&P Global 1200, créé par Standard & Poor's. Le S&P Global 1200[10] est un indice qui facilite la surveillance de la performance des marchés boursiers à l'échelle internationale. Il englobe approximativement 70 % de la capitalisation boursière globale et regroupe sept grands indices régionaux considérés comme des références dans leur zone géographique. On compte parmi ceux-ci la S&P 500 pour les États-Unis, le S&P Europe 350 pour le continent européen, le S&P/TSX 60 pour le Canada, le S&P TOPIX 150 pour le Japon, le S&P/ASX All Australian 50 pour l'Australie, le S&P Asia 50 pour l'Asie et le S&P Latin America 40 pour l'Amérique latine.

L'indice S&P/TSX60[11] englobe 60 des principales entreprises canadiennes, sélectionnées en raison de leur rôle prépondérant dans les secteurs vitaux de l'économie. Il offre aux investisseurs la possibilité de surveiller aisément les performances des grandes entreprises cotées au Canada tout en proposant une méthode économique pour investir sur le marché boursier canadien.

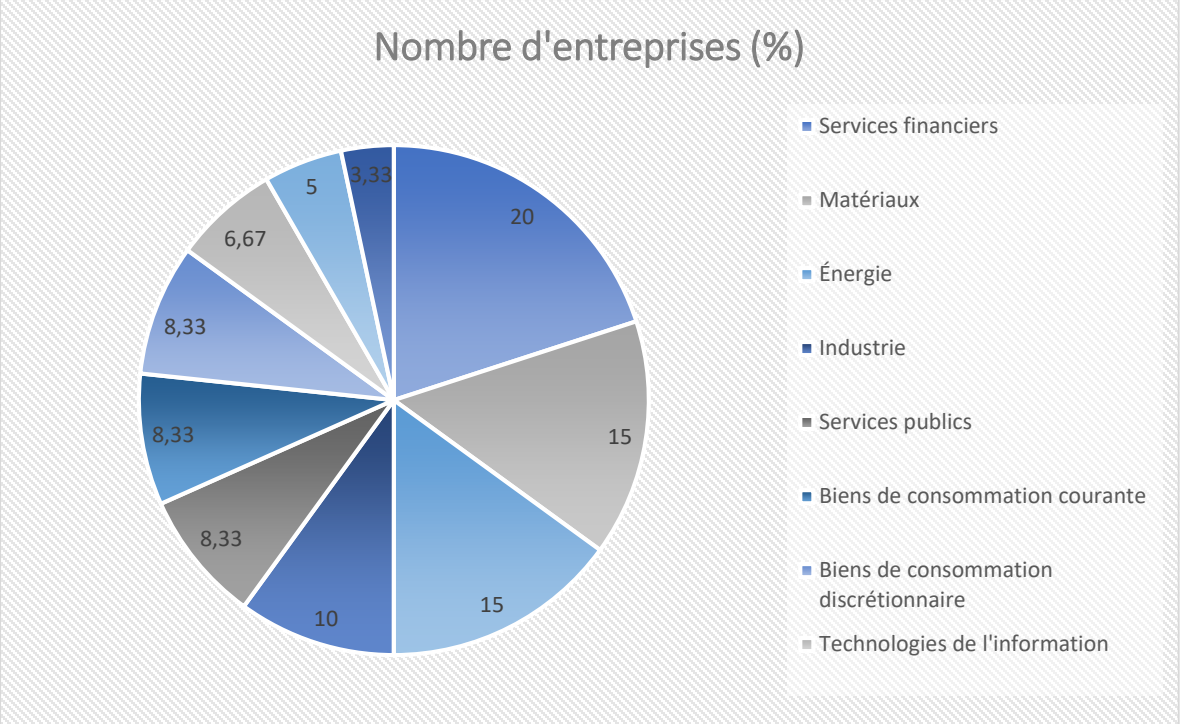
Cela dit, l'étude se focalise sur ces 60 grandes entreprises, car, en accord avec Radu et Smaili (2022), nous estimons que les grandes sociétés sont plus susceptibles de divulguer leurs informations de cybersécurité. De plus ce choix est motivé par le fait qu'étant des entreprises ouvertes, il nous serait plus facile d'accéder aux données.

Notre étude couvre un intervalle de 3 ans allant de 2021 à 2023, aboutissant ainsi à un échantillon final de 180 observations au total. Cette période a été choisie pour analyser les pratiques récentes de divulgation, dans un contexte marqué par une augmentation des risques cybernétiques et une attention accrue des régulateurs. Elle permet également de se distinguer des travaux antérieurs, qui se penchaient souvent sur des données plus anciennes, et d'offrir un aperçu actuel des pratiques des entreprises canadiennes cotées.

La distribution de l'échantillon par secteur d'activité est représentée par le graphique ci-dessous.

[10] https://www.spglobal.com/spdji/en/indices/equity/sp-global-1200/#overview consulté le 2025-05-28

[11] https://tmxinfoservices.com/benchmarks-and-indices/sp-tsx-indices?indexinfo=%5ETX60#tsx consulté le 2025-05-28



Le graphique illustre la prédominance des services financiers, qui comptent pour 20 % des entreprises. Les secteurs du matériel et de l'énergie représentent quant à eux 15 % de l'échantillon. L'industrie et les services publics occupent également une position importante, avec respectivement 10 % et 8,3 %. Les secteurs de la consommation, des technologies de l'information et des communications sont moins représentés, tandis que l'immobilier n'occupe que 3,3 %. Cette répartition sert de base à l'analyse sectorielle de la divulgation en matière de cybersécurité

4.3 Collecte de données.

Les données des 60 entreprises échantillonnées nécessaires à l'étude ont été collectées à partir de différentes sources.

D'une part, les données sur la divulgation de cybersécurité ont été recueillies dans différents rapports et documents réglementaires de formats variés, tels que les formulaires d'information annuelle (AIF), les rapports 40-F, 20-F ou encore les rapports PDF traditionnels déposés sur la plateforme « SEDAR+ » ou publiés sur le site web respectif des entreprises de l'échantillon.

En outre, les données relatives à l'expertise en technologies de l'information des administrateurs ont été collectées dans des circulaires de sollicitation de procurations téléchargées à partir de la base de données « SEDAR+ ». Il s'agit d'un document légal que la loi sur les sociétés et sur les valeurs mobilières oblige à produire lorsqu'on sollicite des procurations pour une assemblée des actionnaires ou pour une assemblée des porteurs de titres avec droit de vote d'un émetteur (Institut canadien des Comptables agréés, 2006).

D'autre part, les données liées aux caractéristiques du conseil d'administration, notamment la taillent, l'indépendance et la diversité, ont été obtenues grâce à la base de données Boardex via WRDS et les autres données, comme le ratio de rentabilité des actifs et le total des actifs nécessaires pour l'analyse quantitative ont été prises sur Compustat.

4.4 Instrument de codage

4.4.1 Fondement de l'instrument de codage

Afin de mesurer la communication faite par les entreprises en matière de cybersécurité, les chercheurs se sont permis d'analyser aussi bien les niveaux de divulgation que la qualité. De ce fait, les approches proposées dans chaque étude diffèrent d'un auteur à un autre.

Parmi les travaux les plus influents, ceux de Héroux et Fortin (2024) ont particulièrement retenu notre attention. Ces autrices ont élaboré une grille de codage composée de 40 éléments regroupés en 7 catégories reflétant les aspects de la divulgation de cybersécurité. Ce sont : les risques, les incidents, les stratégies d'atténuation, la gouvernance, les impacts, les références réglementaires et les autres informations complémentaires. À partir de ces catégories, une analyse manuelle de contenu des notices annuelles, des rapports de gestion annuels et des circulaires de sollicitation de procuration des 250 plus grandes entreprises canadiennes a été effectuée. Cette analyse a ensuite permis d'obtenir des scores qui ont servi à construire un indice de divulgation. Ainsi, avec cette méthode, les autrices ont analysé non seulement la quantité, mais aussi la qualité du contenu des rapports publiés par ces entreprises.

Dans le même ordre d'idées, Firoozi et Mohsni (2023) ont réalisé un indice de divulgation basé sur les lignes directrices de la SEC et de la CSA, ainsi que des entretiens menés avec les spécialistes

du domaine. Les auteurs ont ensuite codé manuellement chaque rapport selon cet indice pour évaluer le niveau de conformité.

Face à cette diversité d'approches, nous avons retenu pour cette étude une méthode regroupant sommairement celles énoncées plus haut. Nous nous sommes inspirés principalement de la grille proposée par Héroux et Fortin (2024), car celle-ci nous semble plus indiquée pour refléter fidèlement le niveau de transparence des entreprises en matière de cybersécurité. Elle présente également l'avantage d'avoir déjà été appliquée au contexte canadien, ce qui en renforce sa pertinence au regard des critères qui ont prévalu dans le choix de notre échantillon composé d'entreprises du TSX60.

4.4.2 Élaboration de l'instrument de codage

L'élaboration de l'instrument de codage repose sur une approche déductive dans laquelle les concepts liés à la cybersécurité ont été déterminés à partir des études antérieures. Il a été question d'identifier les principales catégories en s'inspirant des travaux de Héroux et Fortin (2024). Ainsi, nous distinguons une catégorie principale qui est la divulgation de cybersécurité. À partir de celle-ci, le schéma de codage déductif qui guidera la création de l'instrument de codage a été conçu et comprend nos six sous-catégories qui sont : risques, impact, incidents, mitigation, gouvernance et général (voir Annexe A).

Pour réaliser l'instrument de codage, chaque catégorie a été appréhendée selon des définitions opérationnelles issues des travaux de Héroux et Fortin (2024) et de Firoozi et Mohsni (2023). Les mots-clés liés à la cybersécurité ont été identifiés et regroupés par catégorie (voir Annexe B).

Avec l'instrument de codage obtenu, nous avons procédé à l'analyse de contenu automatisée à l'aide du logiciel Nvivo afin de coder les rapports annuels. Cette approche a été choisie parce que des auteurs comme Allini et al. (2016), Elshandidy et Neri (2015), Gao et al. (2020) ; Li et al., 2018 ; Mazumder et Sobhan, 2021, Saggar et Singh, 2017 cités par Mazumder et Hossain (2023) indiquent que la méthode automatisée est comparativement plus précise et fiable que la méthode manuelle.

Cependant, nous devons admettre que cette méthode ne parvient pas à capturer entièrement le contexte ni la qualité des informations communiquées par les sociétés. Dans cette optique, nous avons procédé à une analyse manuelle du contenu des rapports annuels des entreprises de l'échantillon, qui relèvent du secteur des technologies de l'information. Plus précisément, nous avons effectué une lecture attentive des passages pertinents de ces rapports, en nous concentrant sur les sections traitant des risques, de la gouvernance et des technologies de l'information. Cette procédure visait à valider les occurrences identifiées par le codage automatisé, en distinguant les divulgations réelles en matière de cybersécurité des mentions à caractère descriptif ou commercial, notamment lorsque les termes utilisés renvoient aux produits ou services offerts par ces entreprises. Cette démarche a permis de valider la pertinence de la grille de construction du score de divulgation en comparant les résultats du codage automatisé à une analyse qualitative des divulgations, tout en identifiant certaines limites liées à l'utilisation de mots-clés. Ainsi, cette étape contribue à assurer la fiabilité du contenu de l'instrument de mesure utilisé.

4.5 Analyse de contenu semi-automatique des rapports annuels

L'office québécois de la langue française (1982) définit l'analyse de contenu comme « une étude qui vise à mettre en lumière les données ou informations contenues dans un acte de communication ». Dans le cadre de cette étude, il est question des informations de cybersécurité divulguées dans le rapport annuel des entreprises échantillonnées. L'objectif vise à obtenir des données chiffrées utilisables dans l'analyse quantitative. C'est pourquoi nous avons décidé de créer un indice de divulgation. Comme le souligne Beattie *et al.* (2004), les études portant sur les indices de divulgation s'appuient sur les principes de l'analyse de contenu, laquelle vise à organiser et classifier les segments de texte selon des catégories prédéfinies.

Nous avons procédé à l'analyse directe sommative de contenu par une recherche des occurrences des mots-clés des rapports annuels assistés par le logiciel NVivo 15. La première étape a été de télécharger en format PDF les rapports annuels des entreprises du TSX60 pour les années 2021, 2022 et 2023 et de les importer dans Nvivo. Ensuite, six codes prédéfinis représentant nos six catégories ont été créés dans le logiciel. Rappelons que chaque catégorie est associée à une série de mots-clés.

Pour continuer, avec la fonction « recherche textuelle » de Nvivo, les mots-clés pertinents (non généraux) ont été repérés automatiquement dans les rapports et rattachés aux codes correspondants. Une fois le codage terminé, nous avons utilisé la fonction « croisement matriciel » de Nvivo pour générer un tableau récapitulatif indiquant pour chaque entreprise le nombre total de mots liés à la cybersécurité.

Enfin, ce tableau a été exporté dans Excel en vue d'un retraitement. Ainsi, pour chaque entreprise, nous avons additionné le nombre total de mots-clés identifiés par catégories et le résultat obtenu correspond au score ou encore à l'indice de divulgation en matière de cybersécurité de cette entreprise. L'annexe C présente les entreprises du TSX60 et les scores respectifs de chacune d'elles.

4.6 Modèle de régression

Pour tester les hypothèses de recherche sur les caractéristiques du conseil d'administration, et notamment sa taille, son indépendance, sa diversité et son expertise en technologies de l'information, en tant que déterminants de la divulgation de cybersécurité, deux modèles de régression ont été utilisés en fonction du fait que la variable dépendante soit binaire ou continue.

4.6.1 Régression logistique multiple : présence de divulgation

Un modèle de régression logistique multiple est mobilisé pour analyser la variable dépendante qui est une variable binaire « dummy variable » indiquant la présence ou l'absence d'informations liées à la cybersécurité dans le rapport annuel. Il s'agit d'un test reposant sur une mesure alternative permettant d'identifier les facteurs susceptibles d'influencer la probabilité qu'une entreprise communique sur les enjeux de la cybersécurité. À cette fin, le modèle logistique retenu pour cette première analyse se présente comme suit :

$$\textbf{Logit(PresDivCyb)} = \alpha + \beta_1 \textbf{*TailCA} + \beta_2 \textbf{*IndCA} + \beta_3 \textbf{*DiverCA} + \beta_4 \textbf{*ExpCA} + \beta_5 \textbf{*TailEnt} + \beta_6 \textbf{*Indus} + \beta_7 \textbf{*Rent} + \beta_8 \textbf{*Année\_1} + \beta_9 \textbf{*Année\_2} + \varepsilon \quad \textbf{(1)}$$

Avec

- Logis (PresDivCyb) représentant la transformation logistique de la probabilité que l'entreprise communique sur la cybersécurité.
- IndCA représentant l'indépendance du conseil ;
- DiverCA représentant la diversité de genre au sein du conseil ;
- TailCA représentant la taille du conseil ;
- ExpCA représentant l'expertise en technologies de l'information du conseil ;
- TailEnt représentant la taille de l'entreprise ;
- Indus représentant l'industrie ;
- Rent représentant la rentabilité ;
- Année_1, Année_2 représentants respectivement 2021 et 2022 ;
- α, β1, β2, β3, β4, β5, β6, β7, β8, β9 les constantes ;
- ε le terme d'erreur.

Cependant, cette première analyse ne couvre pas en réalité l'étendue ou le niveau de la divulgation. C'est justement la raison pour laquelle nous avons retenu un second modèle de régression pour proposer une analyse plus approfondie.

4.6.2 Régression linéaire multiple : niveau de divulgation

Nous avons mobilisé une régression linéaire multiple (Ordinary Least Squares : modèle OLS) en utilisant une mesure plus détaillée de la divulgation, soit un score de divulgation obtenu grâce à un instrument de codage quanti-quali. L'utilisation d'un modèle OLS est ici pertinente dans la mesure où le score est une variable continue. Ce deuxième modèle vise à approfondir l'analyse et à confirmer ou rejeter les hypothèses de recherche. Il se présente comme suit :

$$\mathbf{DivCyb = \alpha + \beta_1 * TailCA + \beta_2 * IndCA + \beta_3 * DiverCA + \beta_4 * ExpCA + \beta_5 * TailEnt + \beta_6 * Indus + \beta_7 * Rent + \beta 8 * Année\_1 + \beta 9 * Année\_2 + \varepsilon} \quad \mathbf{(2)}$$

Avec

- DivCyb représentant la divulgation de cybersécurité dans le rapport annuel ;
- IndCA représentant l'indépendance du conseil ;

- DiverCA représentant la diversité de genre au sein du conseil ;
- TailCA représentant la taille du conseil ;
- ExpCA représentant l'expertise en technologies de l'information du conseil ;
- TailEnt représentant la taille de l'entreprise ;
- Indus représentant l'industrie ;
- Rent représentant la rentabilité ;
- Année_1 et Année_2 correspondent respectivement à 2021 et 2022 ;
- α, $\beta 1$, $\beta 2$, $\beta 3$, $\beta 4$, $\beta 5$, $\beta 6$, $\beta 7$, $\beta 8$, $\beta 9$ les constantes ;
- ε le terme d'erreur.

4.7 Définition et mesure des variables

Pour cette étude, les variables retenues ont été opérationnalisées en vue de procéder à l'analyse statistique. Nous distinguons deux catégories de variables : la variable dépendante, qui est un indicateur de divulgation en matière de cybersécurité, et les variables explicatives, qui sont les caractéristiques du conseil d'administration, notamment la taille, l'indépendance, la diversité, et l'expertise en technologies de l'information.

4.7.1 Variable dépendante

La divulgation liée à la cybersécurité a été mesurée de deux façons complémentaires suivantes :

- La présence de divulgation (PresDivCyb) : il s'agit d'une variable binaire qui indique simplement si l'entreprise mentionne ou non la cybersécurité dans son rapport annuel. Elle prend la valeur 1 lorsqu'au moins un mot-clé spécifique lié à la cybersécurité est détecté. Dans le cas contraire, elle prend la valeur 0. Cette mesure permet d'identifier les entreprises qui abordent le sujet, même de manière minimale.
- Score de divulgation (DivCyb) : cette deuxième mesure, plus détaillée, permet de déterminer le niveau d'informations communiquées par les entreprises en matière de cybersécurité.

4.7.2 Variables indépendantes

Les caractéristiques du conseil d'administration retenues comme variables explicatives de la divulgation de cybersécurité des entreprises sont :

- Taille du conseil (TailCA) : nombre total de membres siégeant au conseil d'administration.
- Proportion d'administrateurs indépendants (IndCA) : pourcentage de membres considérés comme indépendants.
- Diversité de genre du conseil (DiverCA) : mesurée à partir du pourcentage de femmes au sein du conseil.
- Expertise en technologies de l'information (ExpCA) : variable binaire codée 1 si au moins un membre du conseil possède une expertise formelle en cybersécurité, informatique ou 0 pour le contraire.

4.7.3 Variables de contrôle

Quatre variables de contrôle qui ont été déjà testées en tant que déterminants de la divulgation dans des recherches antérieures (comme celle de Smaili et al., 2023) ont été intégrées aux modèles afin de tenir compte des caractéristiques structurelles susceptibles d'influencer la divulgation de cybersécurité. Il s'agit de :

- La taille de l'entreprise (TailEnt) : mesurée par le logarithme des actifs totaux.
- La rentabilité (Rent) : mesurée à l'aide du ratio de rentabilité des actifs (ROA)
- Le secteur d'activité (Indus) : Comme notre échantillon comprend des entreprises opérant dans dix secteurs différents, nous avons ajouté neuf variables muettes (ou « dummies ») dans nos modèles pour contrôler l'influence de l'appartenance sectorielle. Nous obtenons ainsi les valeurs dichotomiques suivantes représentant la variable « Secteur d'Activité (Indus) »
    - Indus 1 (Services financiers) = 1 si l'entreprise appartient au secteur des services financiers, sinon 0
    - Indus 2 (Matériaux) = 1 si l'entreprise appartient au secteur des matériaux, sinon 0

- Indus 3 (Énergie) = 1 si l'entreprise appartient au secteur de l'énergie, sinon 0
- Indus 4 (Industrie) = 1 si l'entreprise appartient au secteur de l'industrie, sinon 0
- Indus 5 (Services publics) = 1 si l'entreprise appartient au secteur des services publics, sinon 0
- Indus 6 (Biens de consommation courante) = 1 si l'entreprise appartient au secteur des biens de consommation courante, sinon 0
- Indus 7 (Biens de consommation discrétionnaire) = 1 si l'entreprise appartient au secteur des Biens de consommation discrétionnaire, sinon 0
- Indus 8 (Technologies de l'information) = 1 si l'entreprise appartient au secteur des technologies de l'information, sinon 0
- Indus 9 (Télécommunication) = 1 si l'entreprise appartient au secteur des télécommunications, sinon 0
- Enfin toutes les entreprises, dont les neuf variables, sont égales à zéro, appartiennent au secteur immobilier

- L'année (Année_) : Puisque l'étude a recours aux observations couvrant une période de trois ans allant de 2021 à 2023, deux variables muettes ont été introduites pour contrôler l'influence de l'année.
    - Année_1 = 1 : l'observation correspond à l'exercice 2021
    - Année_1 = 0 : l'observation ne correspond pas à l'exercice 2021
    - Année_2 = 1 : l'observation correspond à l'exercice 2022
    - Année_2 = 0 : l'observation ne correspond pas à l'exercice 2022
    - Enfin, toutes les observations dont les deux dummies sont égales à zéro, par conséquent, correspondent à l'exercice 2023.

L'ensemble des variables mobilisées dans cette étude, qu'il s'agisse de la variable dépendante, des variables explicatives ou des variables de contrôle, sont résumées dans le tableau ci-dessous qui précise pour chacune d'entre elles la référence de la mesure retenue.

Tableau 4.1 Description et mesure des variables

Liste des variables	Mesure	Références de la littérature
- **Variable dépendante** **PresDivCyb : Présence ou absence de divulgation de cybersécurité dans le rapport annuel** **DivCyb : Divulgation relative à la cybersécurité dans le rapport annuel**	Variable binaire égale à un pour les informations de cybersécurité divulguées et à zéro dans le cas contraire. Occurrence des mots-clés liée à la cybersécurité dans le rapport annuel donnant lieu à un score de divulgation	(Mazumder et Hossain, 2023 ; Smaili *et al.*, 2023)
- **Variables indépendantes** **TailCA : La taille du conseil fait référence au nombre total de membres siégeant au conseil d'administration** **IndCA : L'indépendance du conseil reflète le pourcentage de membres du conseil qui ne sont ni employés ni affiliés à la direction de l'entreprise** **DiverCA : La diversité de genre correspond à la proportion de femmes siégeant au conseil d'administration** **ExpCA : L'expertise en technologies de l'information du conseil reflète les compétences techniques en cybersécurité ou en informatique**	Nombre total de membres au sein du conseil d'administration Pourcentage de membres indépendants au sein du conseil Pourcentage de femmes au sein du conseil Variable binaire qui prendra la valeur 1 si un administrateur possède une compétence technique et 0 dans le cas contraire	(Héroux et Fortin, 2024)
- **Variables de contrôles** **Tail_Ent : La taille de l'entreprise désigne la dimension d'une entreprise.** **Indus : Le secteur d'activité désigne la catégorie industrielle ou commerciale**	Logarithme des actifs totaux	(Radu et Smaili, 2022)

dans laquelle l'entreprise opère, en fonction de ses activités principales **Rent : La rentabilité fait référence à la capacité d'une entreprise à générer des profits par rapport à ses coûts et à ses actifs**	Neuf variables muettes pour dix secteurs d'activité Retour sur actifs (ROA) : Résultat net divisé par le total des actifs.	

CHAPITRE 5
ANALYSE ET INTERPRÉTATION DES RÉSULTATS

L'objectif de cette recherche est d'étudier l'influence des caractéristiques du conseil d'administration sur la divulgation en matière de cybersécurité des entreprises. Dans les chapitres précédents, il a été question de présenter la revue de littérature et le cadre théorique se rapportant au sujet, formuler les hypothèses de recherche et décrire la méthodologie retenue pour les analyses statistiques.

Dans ce dernier chapitre, nous exposerons les résultats issus des analyses de régressions logistiques et linéaires effectuées à l'aide de SPSS (Statistical Package for the Social Sciences) et procéderons par la suite à leur interprétation. Enfin, au moyen d'une discussion, nous serons en mesure de confirmer ou de rejeter les hypothèses de recherche et comparer les résultats avec celles issues des études antérieures.

5.1 Statistiques descriptives

L'échantillon comprend 60 sociétés du TSX60, intervenant dans 10 secteurs d'activité distincts, dont les données recueillies vont de 2021 à 2023, donnant lieu à un total de 180 observations (entreprise-année). Le tableau 4.1 présente la distribution de l'échantillon par secteur d'activité.

Tableau 5.1 : Distribution de l'échantillon par industrie

Code du secteur (Indus)	Secteur	N	%
1	Services financiers	36	20,0%
2	Matériaux	27	15,0%
3	Énergie	27	15,0%
4	Industrie	18	10,0%
5	Services publics	15	8,3%
6	Biens de consommation courante	15	8,3%

7	Biens de consommation discrétionnaire	15	8,3%
8	Technologies de l'information	12	6,7%
9	Télécommunication	9	5,0%
10	Immobilier	6	3,3%
	Total	**180**	**100%**

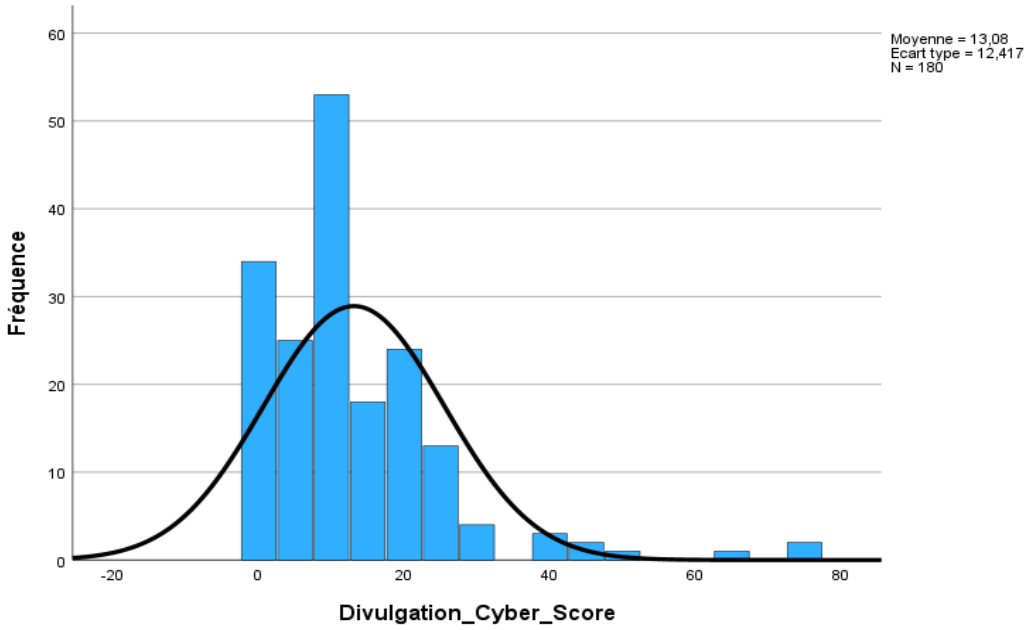
Le secteur des services financiers regroupe à lui seul 20 % des entreprises. Les secteurs du matériel et de l'énergie occupent 15 % de l'échantillon, suivis par l'industrie (10 %) et les services publics (8,3 %). Les secteurs de la consommation, des technologies de l'information et des communications sont moins bien représentés, tandis que l'immobilier ne compte que pour 3,3 %.

Tableau 5.2: Statistiques descriptives

Variables	**N**	**Moyenne**	**Médiane**	**Écart-type**	**Minimum**	**Maximum**
PresDivCyb	180	0,93	1	0.25	0	1
DivCyb	180	13,08	10	12,42	0	76
TailCA	180	11,67	12	2,40	7	17
IndCA	180	82,32%	87,5%	11,80%	45%	100%
DiverCA	180	36,45%	36,40%	8,55%	8,55%	60,00%
ExpCA	180	0,87	1	0,34	0	1
Tail_Ent	180	10,78	10,54	1,54	8,06	14,51

Rent	180	4,66	4,34	3,58	-4,27	21,50

Figure 5.1: Distribution du score de divulgation en cybersécurité (DivCyb).



Les statistiques descriptives montrent une forte présence de la divulgation en matière de cybersécurité dans l'échantillon ; soit une présence moyenne de 93%. Néanmoins, le niveau de la divulgation varie énormément (de 0 à 76) avec un score moyen de 13,08, un écart-type relativement élevé de 12,42. Cela indique que les scores sont très dispersés autour de la moyenne. Ce qui traduit le fait que certaines sociétés communiquent très peu sur leur cybersécurité, tandis que d'autres publient des rapports plus détaillés.

Pour ce qui est des caractéristiques de gouvernance, les conseils comptent en moyenne 12 administrateurs, dont 82% sont indépendants et 36% des femmes, traduisant un certain degré de diversité de genre, même s'il n'est pas élevé. De plus, en moyenne, 87% des conseils disposent d'un expert en technologies de l'information et l'écart-type s'élevant à 0,34 est synonyme d'une faible variabilité.

En outre, les variables de contrôle révèlent une dispersion modérée de la taille des entreprises, soit un écart-type de 1,54, mais une forte dispersion des rentabilités, allant de pertes (minimum -4,27 %) à des rendements élevés (maximum 21,5 %).

Comme mentionné plus haut, les scores de divulgation de cybersécurité sont très dispersés autour de la moyenne. La figure 4.1 est une illustration visuelle montrant que la variable est biaisée à droite. Cela dit, la majorité des entreprises obtiennent des scores entre 0 et 25, tandis qu'une minorité se distingue par des niveaux beaucoup plus élevés. Ce qui confirme le fait que certaines entreprises du TSX60 communiquent plus d'informations sur leur cybersécurité que d'autres.

Pour remédier à cette dispersion asymétrique et rapprocher la variable d'une distribution normale, une transformation logarithmique (ln [DivCyb + 1]) a été appliquée. Cette approche est cohérente avec les pratiques méthodologiques utilisées dans la littérature sur la divulgation comptable. Elle permet de stabiliser la variance et de simplifier l'interprétation des coefficients dans les modèles de régression, comme le montre l'étude de Thomas et al. (2022).

5.2 Résultats de la régression logistique

Le modèle de régression logistique reposant sur une mesure alternative (présence ou absence) est utilisé en amont pour identifier les facteurs pouvant influencer la probabilité qu'une entreprise divulgue sur sa cybersécurité. Les résultats résultants de cette première analyse sont ainsi présentés.

5.2.1 Ajustement du modèle

Tableau 5.3: Ajustement et qualité du modèle logistique

Indicateur	**Khi-carré**	**Ddl**	**Sig. / Valeur**
Test composite des coefficients du modèle	55,186	15	<0,001
Test d'Hosmer et Lemeshow	0,012	8	1,000
Log de vraisemblance -2	-	-	32,989

R-deux de Cox et Snell	-	-	0,264
R-deux de Nagelkerke	-	-	0,682
Pourcentage global -Table de classification	-	-	95,6%

Les résultats présentés dans le tableau 4.3 montrent que le modèle s'ajuste correctement aux données. En effet, le test composite des coefficients du modèle ($Khi^2 = 55,186$; ddl = 15 ; $p < 0,001$) indique que l'ensemble des variables introduites améliore significativement la prédiction de la divulgation de cybersécurité. En outre, le R-deux de Nagelkerke qui mesure le pouvoir explicatif s'élève à 0,682; ce qui signifie que le modèle explique environ 68,2 % de la variance de la variable dépendante. Nous rappelons « qu'une valeur plus élevée du R^2 de Nagelkerke, plus proche de 1, suggère un meilleur ajustement du modèle» [12] . Le R-deux de Cox et Snell expliquent environ 26,4 % de cette variance.

De plus le test d'Hosmer et Lemeshow n'est pas significatif (p = 1,000), ce qui stipule que les probabilités estimées par le modèle concordent avec les données observées. Enfin, le pourcentage global dans la table de classification révèle que le modèle est correct dans 95,6% des cas. En d'autres termes, si une entreprise présente les caractéristiques énumérées dans le modèle (les variables indépendantes), elle sera correctement classée comme divulguant ou non des informations sur la cybersécurité dans 95,6 % des cas. On peut conclure que le modèle démontre une forte capacité prédictive.

5.2.2 Prédicteurs du modèle

Tableau 5.4: Résultats des prédicteurs du modèle logistique

Variable	B	Wald	Sig. (p)	Exp(B)/OR	IC 95 % [Inf – Sup]
TailCA	-0,076	0,239	0,844	0,927	[0,433 – 1,981]

[12] https://spss.espaceweb.usherbrooke.ca/interpretation-26/ , consulté le 2025-09-24

IndCA	0,034	0,250	0,617	1,034	[0,906 – 1,180]
DiverCA	0,310	4,988	**0,026**	1,363	**[1,039 – 1,789]**
ExpCA	0,632	0,560	0,611	1,882	[0,165 – 21,521]
Rent	0,072	0,218	0,728	1,074	[0,717 – 1,611]
Tail_Ent	-0,315	0,662	0,416	0,729	[0,341 – 1,560]
Année_1 (2021)	1,312	0,556	0,456	3,712	[0,118 – 116,735]
Année_2 (2022)	2,015	2,240	0,134	7,499	[0,536 – 104,925]

Rappelons que dans le cadre d'un modèle logistique, l'intervalle de confiance s'interprète à partir du rapport de cote (Exp(B)). Ainsi, un effet est significatif lorsque l'intervalle de confiance (IC) n'inclut pas la valeur 1, qui correspond à l'absence d'effet (Exp (0) =1). Pour variables dont l'IC inclut 1, le résultat est considéré comme non significatif [13].

Ainsi de l'analyse des prédicteurs, on retient que seule la diversité du conseil d'administration ressort significative (B = 0,310; p = 0,026), avec un rapport de cote (Exp(B) = 1,363) et l'IC n'inclut pas la valeur 1 ([1,039 – 1,789]). L'effet est positif, ce qui suggère que plus le conseil compte de femmes en son sein, plus la probabilité de l'entreprise de publier des informations sur la cybersécurité augmente.

En revanche, la taille du conseil (B = -0,076 ; p = 0,844), le niveau d'indépendance (B = 0,034; p = 0,617) et l'expertise en technologies de l'information des administrateurs (B = 0,632; p = 0,611) ne présentent aucun effet significatif.

Dans le même sens, les variables de contrôle, notamment la rentabilité (B = 0,072; p = 0,728), la taille de l'entreprise (B = -0,315 ; p = 0,416) ne ressortent significatives. L'année 2022 (B = 2,015 ;

[13] https://stats.oarc.ucla.edu/spss/output/logistic-regression/?utm_source=chatgpt.com , consulté le 2025/11/26

OR = 7,499) montre une tendance positive, mais non significative (p = 0,134). Aussi, comme le montre le tableau 4.4, les IC des variables non significatives incluent la valeur 1. Ce qui confirme que ces variables n'influencent pas la probabilité de divulguer des informations en cybersécurité.

Les coefficients sectoriels présentent des valeurs extrêmes et des intervalles de confiance qui ne peuvent être interprétés. Par conséquent, ils sont reportés en annexe D.

En conclusion, le modèle logistique met en relief l'effet de la diversité du conseil d'administration comme déterminant significatif, influençant négativement la divulgation en matière de cybersécurité, tandis que les autres variables ne révèlent aucun effet.

La première analyse, qui s'est appuyée sur la régression logistique, a permis d'examiner les facteurs susceptibles d'influencer la probabilité qu'une entreprise divulgue des informations sur sa cybersécurité. Cependant, les résultats ne soutiennent pas nos hypothèses. D'une part, il y a un fort déséquilibre de la variable dépendante « PresDivCyb », caractérisé par la dominance des entreprises divulgatrices (93 % de présence contre 7 % d'absence) ; ce qui peut fausser la capacité de prédiction. D'autre part, l'utilisation d'une mesure binaire de la divulgation ne tient pas compte du niveau ou de la qualité des informations communiquées. Ainsi, pour dépasser ces contraintes et approfondir l'analyse, une régression linéaire multiple est mobilisée afin d'aboutir à des résultats plus concluants.

5.3 Résultats de la régression multiple

Le modèle OSL, qui est basé sur une mesure plus approfondie (score de divulgation), est utilisé en aval pour analyser l'influence des caractéristiques du conseil d'administration (taille, indépendance, diversité et expertise en technologies de l'information de ses membres) sur le niveau de divulgation en matière de cybersécurité. Ainsi, le test de régression linéaire multiple permet d'analyser les relations entre les variables, d'estimer la proportion de variation expliquée par le modèle et d'évaluer la qualité générale de son ajustement aux données.

5.3.1 Vérification des conditions d'applications du test

Avant de présenter les résultats de la régression multiple, les conditions d'application du test ont été vérifiées.

- Homoscédasticité : l'analyse du nuage de points du croisement entre les valeurs prédites standardisées et les résidus standardisés révèle une distribution symétrique des points, qui ont tendance à se rassembler au centre, sans qu'on puisse distinguer de modèle clair. En conclusion, la condition est remplie.

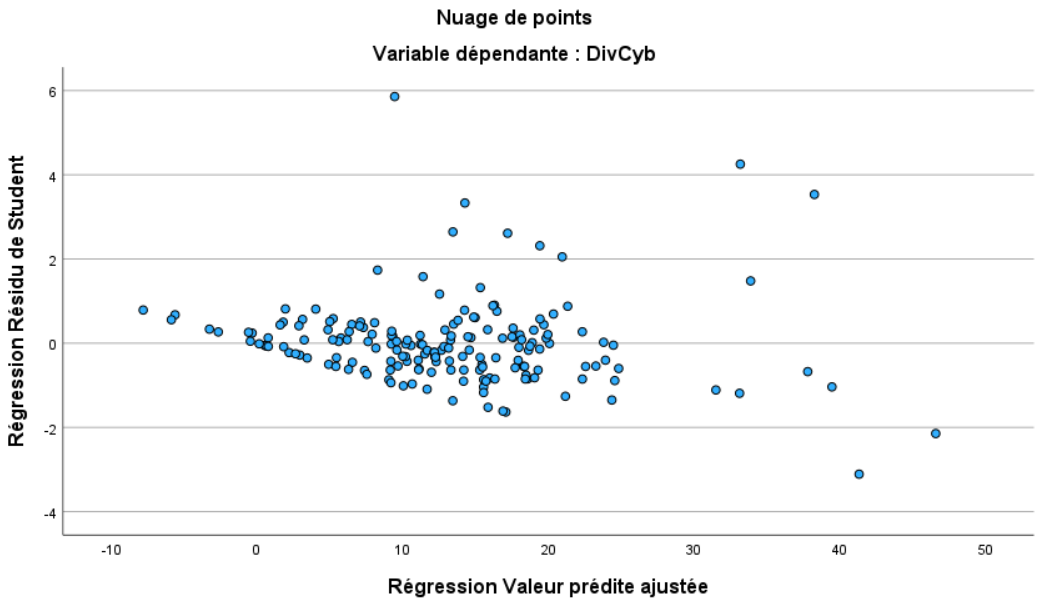


Figure 5.2: Distribution des résidus standardisés (DivCyb)

- Distribution normale et aléatoire des résiduels : la différence entre le modèle et les valeurs observées est près de zéro. Le graphique suivant montre que la distribution des résidus standardisés est à peu près normale.

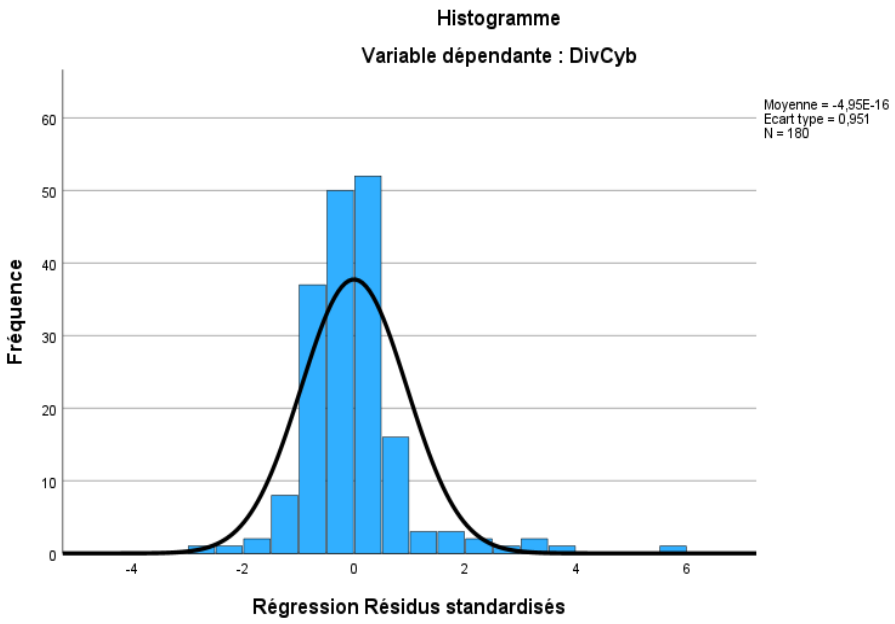


Figure 5.3: Histogramme des résidus standardisés (DivCyb)

- Homogénéité des variances : la variance dans la distribution de la variable dépendante doit être constante pour toutes les valeurs de la variable indépendante. Le graphique ci-dessous présente une distribution symétrique qui se rapproche de la droite, donc la condition est remplie.

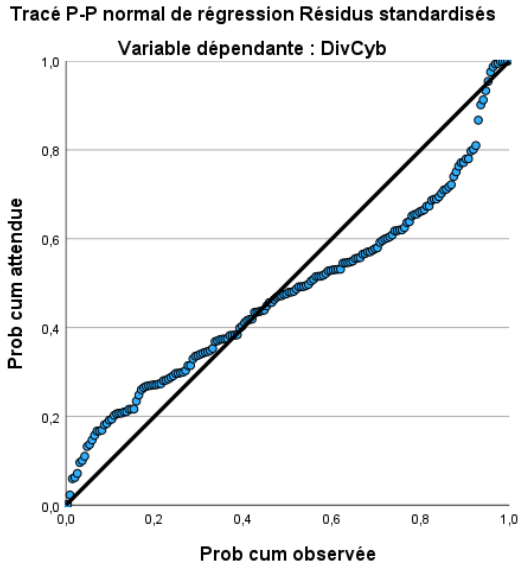


Figure 5.4: Tracé P-P normal des résidus standardisés (DivCyb)

5.3.2 Analyse de corrélation

Tableau 5.5 Matrice de corrélation de Pearson

Matrice de corrélations de Pearson																		
	DivCyb	*Taille_CA*	*IndCA*	*DiverCA*	*ExpCA*	*ROA*	*TailEnt*	*Année_1*	*Année_2*	*Indus 2*	*Indus 5*	*Indus 6*	*Indus 1*	*Indus 9*	*Indus 4*	*Indus 3*	*Indus 7*	*Indus 8*
DivCyb	1,000																	
Taille_CA	0,073	1,000																
IndCA	**0,168**	**-0,170**	1,000															
DiverCA	**0,178**	-0,097	**0,291**	1,000														
ExpCA	**0,337**	0,104	0,089	0,117	1,000													
ROA	**-0,128**	0,008	**-0,223**	**-0,379**	-0,002	1,000												
TailEnt	**0,125**	**0,301**	-0,017	0,119	0,090	**-0,338**	1,000											
Année_1	**-0,167**	-0,031	0,021	**-0,191**	**-0,104**	-0,021	-0,033	1,000										
Année_2	-0,062	0,018	-0,021	0,003	0,000	0,102	0,004	**-0,500**	1,000									
Indus 2	**-0,335**	-0,007	-0,020	**-0,205**	-0,430	0,054	-0,026	0,000	0,000	1,000								
Indus 5	0,011	**-0,253**	0,112	**0,274**	0,000	**-0,167**	-0,014	0,000	0,000	**-0,127**	1,000							
Indus 6	**-0,147**	-0,026	**-0,125**	0,102	0,118	0,103	-0,118	0,000	0,000	**-0,127**	-0,091	1,000						
Indus 1	**0,190**	**0,266**	-0,080	**0,263**	**0,196**	**-0,416**	**0,561**	0,000	0,000	**-0,210**	**-0,151**	**-0,151**	1,000					
Indus 9	**0,447**	**0,202**	-0,048	-0,049	0,090	-0,009	0,021	0,000	0,000	-0,096	-0,069	-0,069	-0,115	1,000				
Indus 4	0,105	-0,094	**0,193**	0,072	0,022	0,026	**-0,221**	0,000	0,000	**-0,140**	-0,101	-0,101	**-0,167**	-0,076	1,000			
Indus 3	-0,074	-0,112	**0,162**	**-0,164**	0,119	**0,199**	0,048	0,000	0,000	**-0,176**	**-0,127**	**-0,127**	**-0,210**	-0,096	**-0,140**	1,000		
Indus 7	-0,056	0,008	-0,058	**-0,264**	0,118	**0,290**	**-0,197**	0,000	0,000	**-0,127**	-0,091	-0,091	**-0,151**	-0,069	-0,101	**-0,127**	1,000	
Indus 8	0,070	0,093	**-0,166**	-0,051	0,039	0,065	**-0,161**	0,000	0,000	-0,112	-0,081	-0,081	**-0,134**	-0,061	-0,089	-0,112	-0,081	1,000

* Gras = significativité

Rappelons que :
DyvCyb correspond à la divulgation de cybersécurité
Année_1 et Année_2 correspondent respectivement aux exercices 2021 et 2022. L'année de référence correspond à l'exercice 2023. Indus un à neuf correspond respectivement aux secteurs des services financiers, des matériaux, de l'énergie, de l'industrie, des services publics, des biens de consommation courants et discrétionnaires, des technologies de l'information et des télécommunications. L'industrie de référence correspond au secteur immobilier.

Le tableau 4.5 présente les coefficients de corrélation entre les variables du modèle. Ainsi, l'examen de la matrice de corrélation indique que la divulgation en matière de cybersécurité est positivement et significativement associée à la présence d'administrateurs indépendants (r = 0,168), à la diversité de genre (r = 0,178) et à la présence d'administrateurs ayant une expertise en technologies de l'information (r = 0,337). Ces résultats semblent suggérer que les entreprises disposant de membres indépendants, d'une large proportion de femmes et d'experts en TI au sein de leur conseil d'administration sont plus enclines à publier des informations sur la cybersécurité, en accord avec nos hypothèses. Cependant, la taille du conseil (r = 0,073) présente une faible corrélation, mais non significative, avec la divulgation.

En outre, on note une faible corrélation positive de la divulgation avec le secteur des services financiers (r = 0,190) et la taille de l'entreprise (r = 0,125). Le secteur des télécommunications (r = 0,447) révèle une forte corrélation positive avec la divulgation de cybersécurité ; ce qui suggère que les entreprises intervenant dans les secteurs les plus exposés aux enjeux technologiques communiquent plus sur la cybersécurité. En revanche, les variables comme le secteur des matériaux (r = -0,335) et, de la consommation courante (r = -0,147), et la rentabilité (r = -0,128) indiquent une corrélation négative.

5.3.3 Analyse de la qualité et de l'ajustement du modèle de régression

Tableau 5.6: Ajustement du modèle de régression aux données

Récapitulatif des modèles [b]

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation	Modifier les statistiques					Durbin-Watson
					Variation de R-deux	Variation de F	ddl1	ddl2	Sig. Variation de F	
1	,695[a]	0,484	0,429	9,379	0,484	8,925	17	162	0,000	1,680
2	,799[a]	0,638	0,600	0,669	0,638	16,775	17	162	0,000	1,339

a. Prédicteurs : (Constante), Tail_Ent, Année_2, Indus 1, Indus, Indus 3, Indus 4, Indus 5, Indus 6, Indus 7, Indus 8, Indus 9

b. Variable dépendante : 1- DivCyb et 2- DivCyb_2

* Modèle 1 : sans transformation de la variable
* Modèle 2 : avec transformation logarithmique

* Rappelons que :

- Année_1 et Année_2 correspondent respectivement aux exercices 2021 et 2022; et l'année de référence correspond à l'exercice 2023,
- Indus 1 à 9 correspondent respectivement aux secteurs des services financiers, des matériaux, de l'énergie, de l'industrie, des services publics, des biens de consommation courantes et discrétionnaires, des technologies de l'information et des télécommunications. L'industrie de référence correspond au secteur immobilier.
- DivCyb correspond à la divulgation de cybersécurité brute
- DivCyb_2 correspond à la divulgation de cybersécurité avec transformation logarithmique

Deux modèles ont été estimés afin de comparer l'ajustement obtenu avec la variable dépendante brute (DivCyb) et sa version transformée logarithmiquement (DivCyb_2 = Ln (DivCyb + 1). Le premier modèle utilise les scores de divulgation tels quels, tandis que le second repose sur la

variable transformée pour corriger la forte asymétrie observée dans la distribution (voir la figure 5.1). La présentation des deux modèles permet de démontrer l'amélioration de la qualité d'ajustement après transformation.

D'après le récapitulatif des modèles, le coefficient de corrélation R (0,695) dans le modèle 1 passe à R (0,799) dans le modèle 2 ; indiquant que les données sont très bien ajustées au modèle. Cela traduit par conséquent une relation relativement forte entre l'ensemble des variables explicatives et la divulgation de cybersécurité. La proportion de la variabilité de la variable dépendante expliquée par le modèle 1 est de 48,3% (R2) comparativement au modèle 2 qui est de 63,8. Le R2 ajusté (0,600) du modèle 2 indique une estimation de la robustesse du modèle à la sélection d'un autre échantillon de la population par rapport à celui du modèle 1 (0,429). L'erreur standard de l'estimation étant l'écart-type de la variation des observations autour de la droite de régression se trouve fortement réduite (9,379 contre 0,669).

Le test de Durbin-Watson suggère dans le modèle 1 une absence d'autocorrélation des résidus, avec une valeur de 1,680 se situant entre 1,5 et 2,5. Contrairement au modèle 2, où cette valeur (1,339) est inférieure à 1,5. Ce résultat traduit donc une autocorrélation des résidus ; autrement dit, les erreurs du modèle présentent une certaine interdépendance, ce qui peut affecter la fiabilité des analyses statistiques et constituer une limite.

Toutefois, la variation de F est significative dans les deux modèles ($p < 0,001$), confirmant que l'ajout des variables explicatives améliore significativement le pouvoir explicatif des modèles.

Tableau 5.7 Qualité du modèle de régression multiple (ANOVA)

ANOVA[a]

Modèle		Somme des carrés	ddl	Carré moyen	F	Sig.
1	Régression	13347,311	17	785,136	8,925	<,001[b]
	de Student	14250,439	162	87,966		
	Total	27597,750	179			

2	Régression	129,227	17	7,602	16,775	<,001[b]
	de Student	73,412	162	0,453		
	Total	202,639	179			

a. Variable dépendante : 1- DivCyb et 2- DivCyb_2

b. Prédicteurs : (Constante), Tail_Ent, Année_2, Indus 1, Indus, Indus 3, Indus 4, Indus 5, Indus 6, Indus 7, Indus 8, Indus 9

* Modèle 1 : sans transformation de la variable
* Modèle 2 : avec transformation logarithmique

*Rappelons que :

- Année_1 et Année_2 correspondent respectivement aux exercices 2021 et 2022; et l'année de référence correspond à l'exercice 2023,
- Indus 1 à 9 correspondent respectivement aux secteurs des services financiers, des matériaux, de l'énergie, de l'industrie, des services publics, des biens de consommation courante et discrétionnaire, des technologies de l'information et des télécommunications. L'industrie de référence est le domaine de l'immobilier.
- DivCyb correspond à la divulgation de cybersécurité brute
- DivCyb_2 correspond à la divulgation de cybersécurité avec transformation logarithmique

Le tableau de l'analyse de la variance nous aide à évaluer la qualité d'ajustement du modèle de régression. Les résultats du test ANOVA confirment la significativité ($p < 0,001$) des deux modèles avec une valeur de F de 8,925 pour le premier et de 16,775 pour le second. Cela indique que l'ensemble des variables indépendantes introduites dans les modèles permet de prédire significativement la variation de la divulgation en matière de cybersécurité. En d'autres termes, les deux modèles sont statistiquement significatifs. Aucune variable n'a été exclue du modèle.

Toutefois, le pourcentage de la variance résiduelle dans le modèle 2 (carré moyen = 7,602) est relativement plus faible que celui dans le modèle 1 (carré moyen = 87,966). En effet, plus le pourcentage de la variance résiduelle est faible, plus le modèle est puissant. Par conséquent, nous présentons les résultats de la régression avec l'utilisation de ce modèle.

5.3.4 Paramètres du modèle

Comme les analyses préliminaires montrent que le modèle 2 est plus puissant et offre une meilleure capacité explicative, nous présentons uniquement les résultats de ce dernier pour les tests de régression.

Tableau 5.8 Résultats des coefficients de régression

	Coefficients non standardisés		**Coefficients standardisés**	**t**	**Sig.**
	B	Erreur standard	Bêta		
(Constante)	-0,996	0,702		-1,420	0,158
Année_1	-0,234	0,130	-0,104	-1,803	0,073
Année_2	-0,196	0,125	-0,087	-1,564	0,120
Rent	0,030	0,018	0,102	1,673	0,096
TailEnt	0,047	0,045	0,068	1,053	0,294
Indus 2	-0,666	0,325	-0,224	-2,048	**0,042**
Indus 5	0,556	0,368	0,145	1,510	0,133
Indus 6	0,047	0,375	0,012	0,126	0,900
Indus 1	0,931	0,384	0,351	2,425	**0,016**
Indus 9	1,602	0,410	0,329	3,912	**0,000**
Indus 4	0,650	0,352	0,184	1,845	0,067
Indus 3	-0,225	0,360	-0,076	-0,627	0,532
Indus 7	0,373	0,376	0,097	0,992	0,322
Indus 8	0,992	0,377	0,233	2,634	**0,009**
TailleCA	-0,033	0,024	-0,074	-1,351	0,179
IndCA	0,020	0,005	0,219	3,913	**0,000**
DiverCA	0,008	0,008	0,068	1,097	0,274
ExpCA	0,940	0,192	0,301	4,899	**0,000**

*Rappelons que :

- Année_1 et Année_2 correspondent respectivement aux exercices 2021 et 2022 ; et l'année de référence correspond à l'exercice 2023,
- Indus 1 à 9 correspondent respectivement aux secteurs des services financiers, des matériaux, de l'énergie, de l'industrie, des services publics, des biens de consommation

courante et discrétionnaire, des technologies de l'information et des télécommunications. L'industrie de référence correspond au secteur de l'immobilier.

Les résultats du test de régression sont présentés dans le tableau 4.9. Ainsi, on peut voir que les divulgations des années 2021 (B = -0,234 ; p = -0,073) et 2022 (B = -0,196; p = 0,120) révèlent un coefficient négatif et non significatif, traduisant un volume de divulgation inférieur à 2023. Toutefois, bien que la divulgation semble avoir progressé au fil du temps, les résultats ne confirment pas statistiquement cette évolution.

Les résultats concernant les facteurs de gouvernance révèlent une fois encore que l'indépendance des membres du conseil exerce un effet positif et fortement significatif (B = 0,020 ; p < 0,001) ; ce qui implique que l'indépendance est un déterminant de la divulgation en matière de cybersécurité. De la même manière, à travers le modèle 2, on remarque que l'expertise en technologies de l'information s des membres du conseil apparaît comme un déterminant (B = 0,940 ; p < 0,001) de la divulgation. Autrement dit, la présence d'administrateurs possédant des compétences spécialisées en TI conduit à une plus grande transparence. Néanmoins, la taille du conseil (p = 0,118) et la diversité de genre demeurent non significatives avec un effet négatif pour le premier et positif pour le second. Ce qui signifie que l'importance en nombre du conseil et la proportion de femmes y siégeant ne constituent pas des déterminants de la divulgation de cybersécurité.

Les variables de contrôle, notamment la rentabilité (p = 0,096) et la taille de l'entreprise (p = 0,294), ne sont pas significatives. Ce qui suppose que la divulgation de cybersécurité n'est pas influencée par ces deux facteurs.

En outre, certains facteurs sectoriels apparaissent comme significatifs, avec un effet positif et donc déterminant de la divulgation. Cela dit, les entreprises intervenant dans les secteurs financiers (Indus 1 : p = 0,016), des technologies de l'information (Indus 8 : p = 0,009), et des télécommunications (Indus 9 : p = 0,000) publient plus d'informations sur la cybersécurité. À l'inverse, l'industrie des matériaux montre un effet négatif et significatif (p = 0,042), reflétant un niveau de transparence plus faible.

5.4 Résumé des résultats

Dans l'ensemble, à l'issue de cette section dédiée à la présentation des résultats, voici les points essentiels à retenir. D'abord, dans le modèle de régression logistique, seule la diversité de genre ressort significative avec un effet positif. Ce qui veut dire que plus la diversité du conseil augmente, plus l'entreprise a de probabilité de publier des informations sur la cybersécurité. Ensuite, dans la régression multiple, deux modèles ont été présentés (une avec transformation logarithmique de la variable dépendante et une sans transformation) du fait de la distribution asymétrique de la variable dépendante (DivCyb). En considérant le modèle avec transformation, car plus robuste, les résultats révèlent une influence positive et significative de l'indépendance et de l'expertise en technologies de l'information des membres du conseil d'administration en tant que déterminants de la divulgation de cybersécurité. Mais, aucune influence de sa taille et de sa diversité n'a été détectée. On retient également l'influence significative des industries, comme le secteur des télécommunications, des technologies de l'information et des services financiers sur la divulgation. Enfin, dans toute l'analyse (logistique et multiple) aucun effet statistique des variables de contrôles, notamment la rentabilité et la taille de l'entreprise n'a été prouvé. Ainsi, on peut conclure que nos résultats suggèrent qu'ils ne sont pas des déterminants de la divulgation de cybersécurité.

L'analyse statistique a permis d'identifier les principaux facteurs susceptibles d'influencer la divulgation en matière de cybersécurité des entreprises. La discussion qui va suivre vise à interpréter ces résultats en les rapprochant à la littérature existante et au cadre théorique mobilisé.

5.5 Discussion

Il s'agit maintenant de confirmer les hypothèses sous-jacentes à cette étude à la lumière des résultats issus des tests statistiques et de comparer ces derniers aux conclusions des recherches précédentes.

Nous rappelons que les deux mesures de la divulgation utilisées dans cette étude sont la présence et le niveau de divulgation en matière de cybersécurité. La première capte la décision des entreprises de communiquer ou non sur la cybersécurité, traduisant une première démarche de transparence. En revanche, la deuxième permet d'appréhender l'intensité de cette communication. Ainsi, ces deux mesures reflètent des dimensions complémentaires des pratiques de divulgation,

l'une portant sur l'engagement à communiquer, et l'autre sur la quantité ou l'ampleur de l'information fournie. Le tableau suivant synthétise nos résultats vis-à-vis des hypothèses.

Tableau 5.9 Rapprochements des résultats aux hypothèses

Hypothèse	*Variable*	*Sig*	*Significativité*	*Décision*
H1	Indépendance du conseil (Niveau de divulgation)	0,000	Significatif (p<0,001)	Confirmée
	Indépendance du conseil (Présence de divulgation)	0,617	Non significatif (p > 0,05)	Rejetée
H2	Diversité de genre du conseil (Niveau de divulgation)	0,274	Non significatif (p > 0,05)	Rejetée
	Diversité de genre du conseil (Présence de divulgation)	0,026	Significatif (p<0,05)	Confirmée
H3	Taille du conseil (Niveau de divulgation)	0,179	Non significatif (p > 0,05)	Rejetée
	Taille du conseil (Présence de divulgation)	0,844	Non significatif (p > 0,05)	Rejetée
H4	Expertise en TI du conseil (Niveau de divulgation)	0,000	Significatif (p<0,001)	Confirmée

Expertise en TI du conseil (Présence de divulgation)	0,611	Non significatif (p > 0,05)	Rejetée

Dans l'ensemble, les résultats de cette étude abondent partiellement dans le sens des hypothèses formulées à partir de la littérature antérieure. En premier lieu, l'hypothèse H1 suggérant une relation positive entre l'indépendance du conseil d'administration et le niveau de divulgation en matière de cybersécurité est confirmée. En effet, les résultats indiquent une forte relation positive et significative, confirmant ainsi les conclusions de plusieurs études (Alodat *et al.*, 2024 ; Héroux et Fortin, 2024 ; Mazumder et Hossain, 2023 ; Smaili *et al.*, 2023). En se référant à la théorie du signal mobilisée dans le cadre théorique, les entreprises disposant de membres indépendants cherchent à envoyer des signaux de leur transparence vis-à-vis des parties prenantes ; réduisant ainsi l'asymétrie d'informations. De plus, du point de vue de la théorie des ressources, les administrateurs indépendants sont assimilables à une ressource stratégique pour l'entreprise. Ils contribuent à renforcer la capacité du conseil à surveiller les risques de cybersécurité et assurer la transparence dans la communication des informations à cet effet.

En second lieu, l'hypothèse H2, qui prévoyait une influence positive de la diversité de genre sur la divulgation de cybersécurité a été partiellement confirmée. Un effet statistiquement significatif de cette variable a été mis en évidence seulement sur la décision de publier de l'information sur la cybersécurité. En effet, l'association entre la variable explicative et celle expliquée (le volume de divulgation) est positive, mais pas statistiquement significative (p = 0,274). Ces résultats divergent partiellement des conclusions des études précédentes (Héroux et Fortin, 2024 ; Kurnia et Ardianto, 2024 ; Mazumder et Hossain, 2023 ; Radu et Smaili, 2022), qui ont conclu que la présence de femmes au sein du conseil favorise la transparence et la divulgation en matière de cybersécurité. Ces auteurs expliquent que les administratrices étant davantage plus sensibles aux risques ont tendance à encourager la communication d'informations utiles aux parties prenantes. Toutefois, nos résultats convergent vers ceux de Alodat et al. (2024) ; Shukla et Pandey (2023) selon lesquels la diversité de genre n'influence pas toujours la divulgation de cybersécurité. Cette absence partielle d'impact peut s'expliquer par le fait que la proportion de femmes siégeant au conseil

d'administration des entreprises échantillonnées n'atteint pas la « masse critique » nécessaire à l'observation d'une influence positive, comme le soulignent Radu et Smaili (2022). Aussi, certaines administratrices peuvent se montrer plus prudentes dans la divulgation d'informations sensibles sur la cybersécurité par souci de sécurité. Du point de vue de la théorie du signal, cette relation partielle peut s'expliquer par le fait que certaines caractéristiques observables du conseil, telles que le genre, peuvent influencer la manière dont l'information est produite et communiquée (Spence, 1973). Ainsi, la présence de femmes au sein du conseil peut encourager une première démarche de divulgation afin de projeter une image de transparence auprès des parties prenantes, sans pour autant influencer l'intensité de l'information divulguée. En parallèle, la théorie des ressources suggère que l'impact de cette diversité dépend de son niveau et de son intégration effective dans les processus décisionnels du conseil d'administration.

Pour continuer, contrairement à nos attentes, l'hypothèse H3 qui prédisait un effet positif de la taille du conseil sur la divulgation de cybersécurité est également rejetée ($p > 0,05$). Ces résultats vont dans le sens des observations de Smaili et al. (2023) et Mazumder et Hossain (2023) qui n'ont pas pu prouver l'existence d'un lien significatif entre la taille du conseil et la divulgation. D'après ces auteurs, une augmentation du nombre d'administrateurs ne traduit pas une meilleure surveillance des risques de cybersécurité ou de divulgation en la matière, surtout si la majorité des membres ne disposent pas de compétences spécifiques liées à la cybersécurité. Par ailleurs, un conseil trop large peut parfois être source de difficultés, de coordination et de lenteurs dans la prise de décisions. Par conséquent, la taille, bien qu'elle soit une caractéristique importante du conseil d'administration, n'est pas un déterminant de la divulgation de cybersécurité, sauf peut-être en présence d'autres facteurs, comme l'indépendance ou l'expertise en techniques d'information. Ces résultats peuvent également être interprétés à la lumière de la théorie des ressources, selon laquelle la simple augmentation du nombre d'administrateurs ne constitue pas nécessairement une ressource stratégique si elle ne s'accompagne pas de compétences spécifiques. Par ailleurs, du point de vue de la théorie du signal, la taille du conseil ne semble pas constituer un signal pertinent pour les parties prenantes en matière de cybersécurité.

Enfin, l'hypothèse H4 qui prévoyait une influence positive de l'expertise en technologies de l'information des administrateurs sur la divulgation en matière de cybersécurité est confirmée avec un degré de significativité élevé ($p<0,001$). Par conséquent, les administrateurs disposant d'une

compétence en informatique, cybersécurité ou technologies numériques sont plus susceptibles de contribuer à une divulgation plus détaillée et crédible. Nos observations rejoignent les conclusions de Héroux et Fortin (2024), Shuka et Pandey (2023), Al-Sartawi (2020) qui ont tous démontré que la présence d'experts techniques au sein du conseil d'administration favorise la communication en matière de cybersécurité. En outre, Chen et al. (2022) ont prouvé que les comités d'audit dotés de compétences informatiques sont plus performants dans la supervision des risques technologiques. Selon la théorie des ressources, cette expertise représente un capital humain rare et difficilement imitable, procurant un avantage concurrentiel à l'entreprise. En parallèle, la théorie du signal soutient que la nomination d'administrateurs possédant des compétences techniques envoie un signal fort de crédibilité et de maîtrise des enjeux numériques aux parties prenantes (Héroux et Fortin, 2024).

Pour ce qui est des variables de contrôles, les résultats obtenus révèlent des effets variables en fonction des facteurs, appuyant certaines tendances observées dans la littérature. En effet, les variables temporelles traduisent une progression croissante de la divulgation au fil du temps. Autrement dit, le niveau de divulgation en matière de cybersécurité s'est renforcé en 2023, traduisant une amélioration de la transparence des entreprises canadiennes face aux enjeux de la cybersécurité.

En outre, nos résultats n'ont pas prouvé l'influence positive de taille de l'entreprise sur la divulgation. Cette conclusion diverge de celles de ces études (D'Arcy *et al.*, 2022 ; Mazumder et Hossain, 2023 ; Smaili *et al.*, 2023) qui soutiennent que les grandes entreprises, disposant de ressources financières et humaines plus importantes, sont plus enclines à divulguer plus pour répondre à la pression de leurs parties prenantes. En revanche, nos conclusions rejoignent Chen et al. (2023) qui n'ont pas trouvé d'effet significatif positif de la taille de l'entreprise sur la divulgation. Cette absence de significativité peut s'expliquer par le fait que l'échantillon de l'étude soit constitué uniquement de grandes entreprises dont la taille est relativement similaire ; entrainant la perte de son pouvoir explicatif.

Concernant la rentabilité, les résultats révèlent un effet positif, mais non significatif. Ce qui suggère que les entreprises les plus performantes financièrement ne sont toujours pas celles qui communiquent le plus sur la cybersécurité. Ce résultat confirme celui de D'Arcy et al. (2022),

Mazumder et Hossain (2023) et Signh (2025) sont parvenus à la conclusion qu'il n'y a pas de relations significatives entre la rentabilité et la divulgation. Cela dit, les entreprises rentables pourraient préférer adopter une divulgation prudente afin d'éviter l'exposition des informations sensibles. Toutefois, ce résultat contredit Smaili et al. (2023) qui avait trouvé un effet positif dans le contexte canadien.

Pour terminer, parmi les variables sectorielles, les industries de télécommunication, des services financiers et de technologies de l'information ressortent significatifs ; confirmant ainsi l'influence du secteur d'activité sur le niveau de divulgation. De ce fait, les entreprises intervenant dans les secteurs plus sensibles aux cyberincidents, tels que le secteur des services financiers, des télécommunications, des technologies de l'information, de l'énergie ou des services publics affichent des niveaux de transparence plus élevés, conformément aux conclusions de Smaili et al. (2023) et au rapport PwC (2023). On peut également comprendre cette transparence accrue à la lumière de la théorie du signal, car les entreprises tendent à renforcer progressivement leur communication pour satisfaire les exigences accrues de leurs parties prenantes, tout en envoyant un message fort d'engagement dans un contexte d'incertitude croissante, compte tenu des menaces qui les guettent.

À l'issue de cette discussion, nous retenons que les résultats s'inscrivent dans le contexte des encadrements réglementaires présentés au chapitre 1, où la pression croissante des autorités, telles que la SEC et les autorités canadiennes en valeurs mobilières incite les entreprises à renforcer leur transparence en matière de cybersécurité. Ces autorités, en tant que parties prenantes, jouent un rôle déterminant dans l'évolution des pratiques de divulgation. Ainsi, la divulgation observée peut être perçue non seulement comme le reflet des caractéristiques internes des entreprises, mais également comme une réponse aux attentes réglementaires et des parties prenantes.

CONCLUSION

Ce mémoire avait pour objectif d'explorer les déterminants de la divulgation en matière de cybersécurité, en mettant en lumière l'impact des caractéristiques du conseil d'administration sur la décision de publier et l'étendue des informations divulguées par les entreprises. Il s'est appuyé sur un échantillon de 180 observations (entreprises-années) issues de sociétés canadiennes constituant l'indice S&P/TSX60, sur une période de 3 ans allant de 2021 à 2023. En mobilisant la théorie des ressources et la théorie du signal, cette recherche visait à identifier les facteurs susceptibles d'impacter la divulgation en matière de cybersécurité des entreprises.

À l'issue de l'analyse, les résultats obtenus confirment partiellement nos hypothèses. En effet, l'indépendance et l'expertise en TI du conseil exercent une influence positive et significative sur le niveau de divulgation. De ce fait, les entreprises canadiennes qui disposent de conseil comptant des membres indépendants et qui sont dotés d'une compétence pertinente en TI communiquent plus d'informations sur la cybersécurité. En outre, bien que la présence de femmes au sein du conseil n'impacte pas directement le volume d'informations divulguées par les entreprises, elle détermine néanmoins le choix de celles-ci de publier (ou pas) de l'information concernant la cybersécurité. Ces résultats démontrent l'importance stratégique d'une bonne composition du conseil ; incluant des femmes, des membres indépendants et possédant une expertise en cybersécurité ou TI afin de renforcer la transparence et de répondre aux attentes en informations des parties prenantes.

En revanche, les facteurs comme taille du conseil, la rentabilité et la taille de l'entreprise n'ont démontré aucun effet significatif sur le niveau de divulgation de cybersécurité. Contrairement aux prédictions, les résultats n'ont pas identifié ces facteurs comme déterminants du niveau d'informations publiées sur la cybersécurité par les entreprises canadiennes cotées en bourse.

Par ailleurs, les variables temporelles révèlent une progression graduelle de la divulgation entre les années 2021 et 2023. Au même moment, les variables sectorielles mettent en évidence l'effet positif des industries des télécommunications, des technologies de l'information et des services financiers sur la divulgation. Faisant partie des secteurs sensibles identifiés dans la littérature, les

entreprises y intervenant se distinguent des autres par une communication plus étendue en matière de cybersécurité.

Cette étude apporte une contribution tant à la littérature existante, jusqu'ici peu développée qu'aux pratiques organisationnelles. Sur le plan théorique, elle contribue à l'enrichissement de la littérature sur la divulgation de cybersécurité en mobilisant conjointement la théorie des ressources et celle du signal dans un contexte canadien. Ce mémoire s'inscrit dans la continuité des travaux empiriques réalisés dans le contexte canadien, notamment ceux de Smaili et al.(2023) et de Héroux et Fortin (2024) qui ont mis en évidence le rôle du conseil d'administration dans la divulgation en matière de cybersécurité. Toutefois, elle s'en distingue en proposant une analyse se basant sur des données plus récentes couvrant la période de 2021 à 2023. Les résultats confirment que certaines caractéristiques du conseil d'administration, notamment son indépendance et l'expertise en TI de ses membres, constituent des ressources stratégiques qui influencent l'étendue de la divulgation en matière de cybersécurité ; et sa diversité de genre, la décision des entreprises de communiquer à cet effet. De ce fait, nos conclusions renforcent la perspective de la théorie des ressources selon laquelle la composition du conseil serait une ressource ; un actif à caractère humain qui confère un avantage concurrentiel à l'entreprise la détenant. De plus, nos résultats viennent soutenir la théorie du signal en montrant que les entreprises dont les conseils sont efficacement constitués sont plus disposées à assurer une divulgation plus large et plus transparente dans le but de réduire l'asymétrie d'informations et ainsi prouver leur engagement vis-à-vis des parties prenantes face aux enjeux de la cybersécurité (Héroux et Fortin, 2024 ; Smaili *et al.*, 2023).

Sur le plan méthodologique, ce mémoire apporte une contribution en adoptant une approche mixte combinant l'analyse de contenu automatisé à l'aide de Nvivo pour mesurer la divulgation de cybersécurité et l'utilisation de modèles de régressions logistiques et linéaires multiples pour effectuer les analyses statistiques. De cette manière, il a été possible d'explorer à la fois la présence et le niveau de divulgation.

Sur le plan pratique, cette recherche peut servir de référence pour les investisseurs et les dirigeants d'entreprises, car elle souligne l'importance de promouvoir une composition adéquate du conseil en nommant des f administrateurs indépendants et disposant d'une compétence en technologies de l'information. En effet, ces caractéristiques permettent de renforcer la communication

d'informations en matière de cybersécurité. De plus, les régulateurs pourraient s'appuyer sur nos conclusions pour standardiser la divulgation des entreprises en recommandant une constitution stratégique des conseils.

Malgré les contributions apportées par cette recherche, elle présente certaines limites qu'il convient de relever. Tout d'abord, l'échantillon est composé uniquement de grandes entreprises du TSX60 ; ce qui limite la généralisation des résultats à l'échelle de toutes les tailles d'entreprises. Ensuite, la mesure de la divulgation (fréquence des mots-clés) présente un caractère subjectif. En effet, l'analyse de contenu automatisé utilisée bien qu'étant une méthode rapide, elle peut être moins fiable, car ne permettant pas de cerner le contexte dans lequel ces mots-clés ont été utilisés dans les rapports. De plus, le déséquilibre entre les entreprises divulgatrices et non divulgatrices peut influencer la fiabilité du modèle logistique. Aussi, l'analyse repose principalement sur l'étude des effets individuels des variables, sans considérer leurs interactions potentielles. En outre, le test de Durbin Watson du modèle transformé ne se situant pas dans l'intervalle adéquat (1.5 à 2,5), suggère une autocorrélation des résidus. Ce qui peut entrainer une sous-estimation des erreurs standards, rendant ainsi certains tests de significativité trop optimistes. En outre, le secteur financier représente une part importante de l'échantillon étudié, ce qui peut influencer les résultats en raison de ses particularités réglementaires et de son niveau d'exposition élevé aux risques de cybersécurité. Une analyse complémentaire excluant ce secteur aurait permis de mieux isoler les effets observés et de tester la robustesse des résultats. Finalement, la période d'étude choisie (2021-2023) paraît trop courte pour analyser les tendances à long terme en matière de divulgation.

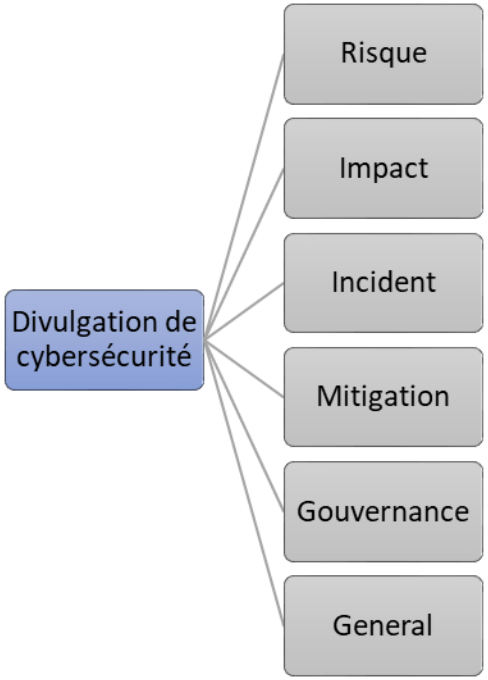
Dans cette perspective, plusieurs pistes de recherche futures peuvent être envisagées. Tout d'abord, il serait pertinent d'approfondir l'analyse en s'intéressant à la nature des informations divulguées, en distinguant notamment les divulgations qualitatives et quantitatives, ou encore inclure une variable distinguant divulgation volontaire vs obligatoire. Ensuite, de futures recherches pourraient adopter une approche fondée sur des configurations combinées de variables, permettant d'analyser la cohérence entre les caractéristiques du conseil d'administration et les pratiques de divulgation, et de mieux articuler les cadres théoriques mobilisés. Par ailleurs, l'intégration d'autres perspectives théoriques, telles que la théorie de la légitimité, permettrait d'enrichir l'analyse en tenant compte des motivations liées aux pressions institutionnelles et réglementaires. Il serait également intéressant d'étendre l'analyse à d'autres contextes géographiques afin de comparer les

pratiques de divulgation à l'échelle internationale. Enfin, des études longitudinales couvrant des périodes plus longues permettraient de mieux comprendre l'évolution des pratiques de divulgation en matière de cybersécurité dans le temps.

En définitive, ce mémoire met en exergue l'importance stratégique de la gouvernance d'entreprise à travers la composition du conseil d'administration face aux enjeux de la cybersécurité et la communication d'informations à cet effet. Dans le contexte actuel où les pressions des parties prenantes continuent de s'accroître en termes de besoins en informations sur leur cybersécurité, la divulgation réactive et proactive d'informations en la matière constitue un signal de crédibilité envers ceux-ci.

ANNEXE A

SCHÉMA DE CODAGE



ANNEXE B

INSTRUMENT DE CODAGE

Codes prédéfinis	Définition	Exemple de mots-clés	Extraits types
RISK	Recense les termes et informations relatifs aux vulnérabilités et menaces pesant sur l'entreprise.	« cyberrisque » « risque de cybersécurité » « risque de sécurité informatique » « menace cybernétique » « attaque d'hameçonnage »	« La cybersécurité et la sécurité infonuagique font partie intégrante des activités commerciales, de la marque et de la réputation de BMO. À mesure que la technologie évolue rapidement et que les capacités de connectivité des appareils numériques se développent, les cybermenaces et les cyberrisques évoluent également. Ces menaces comprennent : les violations ou les perturbations de nos systèmes ou de nos opérations, ainsi que l'accès, l'utilisation ou la diffusion non autorisés de renseignements concernant BMO, nos clients ou nos employés. » (*BMO Financial Group 206th Annual Report 2023 111)*
IMPACT	Regroupe les mentions d'effets potentiels (pertes financières, perturbations opérationnelles,	« violation de données » « perte de données »	« Une violation de nos mesures de cybersécurité ou une défaillance ou un dysfonctionnement de l'un de nos systèmes informatiques, des systèmes de sauvegarde ou de stockage de données associés pourrait entrainer une perturbation d'un ou plusieurs aspects de nos activités et entrainer, entre autres, des pertes financières, une atteinte à notre réputation, une perte d'opportunités commerciales, un détournement ou une divulgation non autorisée d'informations confidentielles ou personnelles, des dommages à nos systèmes et à nos

	atteinte à la réputation)	« accès non autorisé » « interruption d'activité »	partenaires commerciaux, une violation des lois sur la confidentialité et autres lois, des litiges, des sanctions réglementaires et des coûts de réparation et de restauration, ainsi qu'une augmentation des coûts de maintenance de nos systèmes. » *(Brookfield Infrastructure Partners L.P_2023)* « Les pandémies, y compris la pandémie de COVID-19, ont provoqué et pourraient à l'avenir provoquer des perturbations dans nos opérations et celles de nos clients (ce qui pourrait entrainer une augmentation du risque et de la fréquence des incidents de cybersécurité), une volatilité des marchés et des perturbations économiques, qui pourraient nous affecter négativement. » *Fiscal 2021 results- CGI*
INCIDENT	Recense les divulgations relatives aux attaques, violations de données	« cyber incident » « violation de sécurité » « fuite de données » « piratage »	« Les technologies, systèmes et réseaux de la Banque, ceux de ses clients (y compris leurs propres appareils) et ceux des tiers fournissant des services à la Banque continuent d'être exposés à des cyberattaques et peuvent être sujets à des interruptions de services, à des atteintes à la sécurité des données ou à d'autres violations (telles que la perte ou la divulgation d'informations confidentielles, y compris les informations des clients ou des employés), à des vols d'identité, à de l'espionnage industriel ou à d'autres compromissions. La Banque a connu des interruptions de service suite à une défaillance technologique chez un tiers et pourrait être exposée à de telles perturbations à l'avenir en raison de cyberattaques et/ou de défaillances technologiques. » (*TD BANK GROUP ANNUAL REPORT 2023_Page77)*
MITIGATION	Inclut les mesures de défense et de prévention contre les cyber-risques	« chiffrement » « plan de réponse aux incidents » « test d'intrusion »	« Nous estimons que notre programme de cybersécurité est conçu pour protéger efficacement l'intégrité et la disponibilité de nos informations et technologies. Ce programme aborde la gouvernance de la sécurité, la sensibilisation à la sécurité, la formation des employés, la sécurité des accès et des terminaux, la gestion des vulnérabilités, les tests d'intrusion, la surveillance de la sécurité et la réponse aux incidents. Nous utilisons des technologies pour optimiser nos capacités de détection et de réponse aux risques de sécurité, ainsi que les contrôles d'accès et

		« programme de sensibilisation » « évaluation par un tiers »	les protections anti-malware » *(Brookfield Infrastructure Partners L.P_2023 pg 23)* « Nous continuons de renforcer notre cadre de cybercontrôle et d'améliorer nos capacités de résilience et de cybersécurité, notamment grâce à une surveillance 24h/24, à l'analyse des menaces internes et externes par le biais de cyberrenseignements, et à l'alerte en cas d'événements et d'incidents de sécurité potentiellement suspects. » *(Royal Bank of Canada : Annual Report 2023 101)* « Chez BMO, notre réponse comprend des investissements dans notre unité de lutte contre la criminalité financière et notre infrastructure technologique, ainsi que la fourniture à notre équipe des moyens nécessaires pour détecter et contrer les menaces de cybersécurité en Amérique du Nord, en Europe et en Asie afin de nous aider à protéger les données de nos clients et de nos employés. » *(BMO Financial Group 206th Annual Report 2023 111)*
GOUVERNANCE	Couvre les éléments de supervision et de pilotage	« surveillance du conseil d'administration » « comité des technologies»	« CAE a renforcé la surveillance de son conseil d'administration dans les domaines de la planification stratégique, de la gestion des risques d'entreprise aux niveaux opérationnel et organisationnel, de la cybersécurité, de la technologie et des ressources humaines en recommandant l'élection de trois nouveaux administrateurs qui ont déjà apporté une contribution significative depuis leur arrivée au conseil. » (*CAE 2023 Annual Report)* « Le Comité des technologies supervise les différentes composantes du programme technologique de la Banque. Il examine, entre autres, la stratégie technologique de la Banque et surveille les risques technologiques, notamment les cyberrisques, la cybercriminalité et la protection des renseignements personnels. » (*National Bank of Canada 2023 Annual Report 24)*

GÉNÉRAL	Regroupe tous les autres termes liés à la cybersécurité	« cybersécurité » « sécurité de l'information » « sécurité informatique » « sécurité des données » « programme de cybersécurité » « sécurité des réseaux »	« Nous sommes soumis à des lois, réglementations et normes strictes et changeantes en matière de confidentialité, à des politiques de sécurité de l'information et à des obligations contractuelles liées à la confidentialité et à la sécurité des données. Tout manquement, réel ou perçu, à ces obligations pourrait nous exposer à des sanctions gouvernementales et nuire à notre marque et à notre réputation. » (*Fiscal 2022 results- CGI)*

ANNEXE C

SCORE DE DIVULGATION DES ENTREPRISES DU S&P/TSX60

#	Symbole	Nom de l'entreprise	Secteur d'activité	Score de divulgation
1	AEM	Agnico Eagle Mines Limited	Matériaux	2
2	AQN	Algonquin Power & Utilities Corp.	Services publics	37
3	ATD	Alimentation Couche-Tard Inc.	Biens de consommation courante	6
4	BMO	Bank of Montreal	Services financiers	60
5	BNS	Bank of Nova Scotia	Services financiers	62
6	ABX	Barrick Mining Corporation	Matériaux	2
7	BCE	BCE Inc.	Services de communication	160
8	BAM	Brookfield Asset Management Ltd.	Services financiers	39
9	BN	Brookfield Corporation	Services financiers	37
10	BIP.UN	Brookfield Infrastructure Partners L.P.	Services publics	59
11	CAE	CAE Inc.	Industrie	43
12	CCO	Cameco Corporation	Énergie	0
13	CAR.UN	Canadian Apartment Properties Real Estate Investment Trust	Immobilier	26
14	CM	Canadian Imperial Bank Of Commerce	Services financiers	70
15	CNR	Canadian National Railway Company	Industrie	44
16	CNQ	Canadian Natural Resources Limited	Énergie	3
17	CP	Canadian Pacific Kansas City Limited	Industrie	52
18	CTC.A	Canadian Tire Corporation Limited	Biens de consommation discrétionnaire	21
19	CCL.B	CCL Industries Inc.	Matériaux	1
20	CVE	Cenovus Energy Inc.	Énergie	6
21	GIB.A	CGI Inc.	Technologies de l'information	52
22	CSU	Constellation Software Inc.	Technologies de l'information	14
23	DOL	Dollarama Inc.	Biens de consommation discrétionnaire	25
24	EMA	Emera Incorporated	Services publics	30
25	ENB	Enbridge Inc.	Énergie	55
26	FM	First Quantum Minerals Ltd.	Matériaux	0
27	FSV	FirstService Corporation	Immobilier	0
28	FTS	Fortis Inc.	Services publics	44
29	FNV	Franco-Nevada Corporation	Matériaux	0
30	WN	George Weston Limited	Biens de consommation courante	18
31	GIL	Gildan Activewear Inc.	Biens de consommation discrétionnaire	28
32	H	Hydro One Limited	Services publics	33
33	IMO	Imperial Oil Limited	Énergie	119
34	IFC	Intact Financial Corporation	Services financiers	58
35	K	Kinross Gold Corporation	Matériaux	32
36	L	Loblaw Companies Limited	Biens de consommation courante	24
37	MG	Magna International Inc.	Biens de consommation discrétionnaire	21
38	MFC	Manulife Financial Corporation	Services financiers	43
39	MRU	Metro Inc.	Biens de consommation courante	33
40	NA	National Bank of Canada	Services financiers	74
41	NTR	Nutrien Ltd.	Matériaux	31
42	OTEX	Open Text Corporation	Technologies de l'information	76
43	PPL	Pembina Pipeline Corporation	Énergie	22
44	POW	Power Corporation of Canada	Services financiers	25
45	QSR	Restaurant Brands International Inc.	Biens de consommation discrétionnaire	67
46	RCI.B	Rogers Communications Inc.	Services de communication	90
47	RY	Royal Bank of Canada	Services financiers	54
48	SAP	Saputo Inc.	Biens de consommation courante	25
49	SHOP	Shopify Inc.	Technologies de l'information	54
50	SLF	Sun Life Financial Inc.	Services financiers	66
51	SU	Suncor Energy Inc.	Énergie	14
52	TRP	TC Energy Corporation	Énergie	37
53	TECK.B	Teck Resources Limited	Matériaux	1
54	T	TELUS Corporation	Services de communication	85
55	TRI	Thomson Reuters Corporation	Services financiers	52
56	TD	Toronto-Dominion Bank	Industrie	68
57	TOU	Tourmaline Oil Corp.	Énergie	38
58	WCN	Waste Connections Inc.	Industrie	65
59	WPM	Wheaton Precious Metals Corp.	Matériaux	18
60	WSP	WSP Global Inc.	Industrie	34

ANNEXE D

RÉSULTATS COMPLET DES PRÉDICTEURS DU MODÈLE LOGISTIQUE

Variables de l'équation

		B	E.S	Wald	ddl	Sig.	Exp(B)	Intervalle de confiance 95% pour EXP(B)	
								Inférieur	Supérieur
Pas 1[a]	Taille_CA	-,076	,388	,039	1	,844	,927	,433	1,981
	IndCA	,034	,067	,250	1	,617	1,034	,906	1,180
	DiverCA	,310	,139	4,988	1	,026	1,363	1,039	1,789
	ExpCA	,632	1,243	,259	1	,611	1,882	,165	21,521
	ROA	,072	,207	,121	1	,728	1,074	,717	1,611
	TailEnt	-,315	,388	,662	1	,416	,729	,341	1,560
	Indus 2	2,762	1,899	2,116	1	,146	15,832	,383	654,279
	Indus 5	20,715	8558,173	,000	1	,998	991290704,93	,000	.
	Indus 6	22,578	8841,536	,000	1	,998	6391389987,5	,000	.
	Indus 1	24,473	4992,685	,000	1	,996	42524123151	,000	.
	Indus 9	24,171	11350,391	,000	1	,998	31436688229	,000	.
	Indus 4	22,767	7566,943	,000	1	,998	7718979656,8	,000	.
	Indus 3	23,491	6792,941	,000	1	,997	15925407245	,000	.
	Indus 7	26,072	8100,416	,000	1	,997	2,104E+11	,000	.
	Indus 8	22,883	10701,017	,000	1	,998	8668332257,3	,000	.
	Année_1	1,312	1,759	,556	1	,456	3,712	,118	116,735
	Année_2	2,015	1,346	2,240	1	,134	7,499	,536	104,925
	Constante	-12,058	9,040	1,779	1	,182	,000		

a. Introduction des variables au pas 1 : Taille_CA, IndCA, DiverCA , ExpCA , ROA, TailEnt , Indus 2, Indus 5, Indus 6, Indus 1 , Indus 9 , Indus 4, Indus 3, Indus 7, Indus 8 , Année_1, Année_2.

BIBLIOGRAPHIE

2017 Cost of Data Breach Study: United States. (2017, 13 juin). Ponemon Institute. https://www.ponemon.org/news-updates/blog/security/2017-cost-of-data-breach-study-united-states.html

2024 Canada Spencer Stuart Board Index Snapshot. (2024, juin). Spencer Stuart. https://www.spencerstuart.com/research-and-insight/canada-board-index

Abdullah, Maizatulakma, Abdul Shukor, Zaleha, Mohamed, Zakiah Muhammadun et Ahmad, Azlina. (2015). Risk management disclosure: A study on the effect of voluntary risk management disclosure toward firm value. Journal of Applied Accounting Research, 16(3), 400-432. https://doi.org/10.1108/JAAR-10-2014-0106

Al-Maghzom, Abdullah, Hussainey, Khaled et Aly, Doaa. (2017). Value relevance of voluntary risk disclosure levels: evidence from Saudi banks. Accounting and Taxation, 8(1), 1-26.

Alodat, Ahmad Yuosef, Hao, Yunhong, Nobanee, Haitham, Ali, Hazem, Mansour, Marwan et Al Amosh, Hamzeh. (2024). Board characteristics and cybersecurity disclosure: evidence from the UK. Electronic Commerce Research. https://doi.org/10.1007/s10660-024-09867-w

Al-Sartawi, Abdalmuttaleb MA Musleh. (2020). Information technology governance and cybersecurity at the board level. International Journal of Critical Infrastructures, 16(2), 150-161.

Anton, Robert, Wiley, Blair et Kolibar, Danile. (2017). Avis multilatéral 51-347 du personnel des ACVM – Information sur les risques et les incidents liés à la cybersécurité. Osler, Hoskin & Harcourt S.E.N.C.R.L./s.r.l. https://www.osler.com/fr/articles/mises-à-jour/avis-multilateral-51-347-du-personnel-des-acvm-i/

Barney, Jay. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 17(1), 99-120. https://doi.org/10.1177/014920639101700108

Beattie, Vivien, McInnes, Bill et Fearnley, Stella. (2004). A methodology for analysing and evaluating narratives in annual reports: a comprehensive descriptive profile and metrics for disclosure quality attributes. Accounting Forum, 28(3), 205-236. https://doi.org/10.1016/j.accfor.2004.07.001

Beaud, Michel, Gravier, Magali et Toledo, Alain de. (2005). L'art de la thèse : comment préparer et rédiger un mémoire de master, une thèse de doctorat ou tout autre travail universitaire à l'ère du net (Éd. révisée, mise à jour et élargie). La Découverte.

Booto Ekionea, Jean-Pierre, Fillion, Gérard, Bernard, Prosper et Plaisent, Michel. (2011). Les technologies de l'information, la gestion des connaissances et un avantage concurrentiel soutenu : une analyse par la théorie des ressources. Revue de l'Université de Moncton, 41(1), 247-271. https://doi.org/10.7202/1006096ar

Calderon, Thomas G. et Gao, Lei. (2022). Changes in corporate cybersecurity risk disclosures after SEC comment letters. Journal of Accounting and Public Policy, 41(5), 106993. https://doi.org/10.1016/j.jaccpubpol.2022.106993

Chen, Chu, Hartmann, Caroline et Gottfried, Anne. (2022). The impact of audit committee IT expertise on data breaches. Journal of Information Systems, 36(3), 61-81.

Chen, Jing, Henry, Elaine et Jiang, Xi. (2023). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. Journal of Business Ethics, 187(1), 199-224. https://doi.org/10.1007/s10551-022-05107-z

Comerford, Jason et MacDougall, Andrew. (2023, 21 août). Nouvelles règles de la SEC exigeant la publication d'information sur la cybersécurité et répercussions pour les émetteurs canadiens. Osler, Hoskin & Harcourt S.E.N.C.R.L./s.r.l. https://www.osler.com/fr/articles/mises-à-jour/nouvelles-regles-de-la-sec-exigeant-la-publication-d-information-sur-la-cybersecurite-et-repercussio/

Connelly, Brian L., Certo, S. Trevis, Ireland, R. Duane et Reutzel, Christopher R. (2011). Signaling Theory: A Review and Assessment. Journal of Management, 37(1), 39-67. https://doi.org/10.1177/0149206310388419

Cordazzo, Michela, Papa, Marco et Rossi, Paola. (2017). The interaction between mandatory and voluntary risk disclosure: a comparative study. Managerial Auditing Journal, 32(7), 682-714. https://doi.org/10.1108/MAJ-01-2016-1308

CSA Multilateral Staff Notice 51-347 - Disclosure of cyber security risks and incidents. (2017).

D'Arcy, John, University of Delaware, Basoglu, Asli et University of Delaware. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. Journal of the Association for Information Systems, 23(3), 779-805. https://doi.org/10.17705/1jais.00740

Elgammal, Mohammed M., Hussainey, Khaled et Ahmed, Fatma. (2018). Corporate governance and voluntary risk and forward-looking disclosures. Journal of Applied Accounting Research, 19(4), 592-607. https://doi.org/10.1108/JAAR-01-2017-0014

Elnahass, Marwa, Ahmed, Yousry et Trinh, Vu Quang. (2024). Empowering Women to Lead Cybersecurity: The Effect of Female Executives on Disclosure Sentiment. International Journal of Finance & Economics, ijfe.3067. https://doi.org/10.1002/ijfe.3067

Elsayed, Nader et Hassanein, Ahmed. (2024). Is voluntary risk disclosure informative? The role of UK firm-level governance. International Journal of Productivity and Performance Management, 73(6), 1826-1855. https://doi.org/10.1108/IJPPM-09-2022-0486

Elshandidy, Tamer, Fraser, Ian et Hussainey, Khaled. (2013). Aggregated, voluntary, and mandatory risk disclosure incentives: Evidence from UK FTSE all-share companies. International Review of Financial Analysis, 30, 320-333. https://doi.org/10.1016/j.irfa.2013.07.010

Firoozi, Maryam et Mohsni, Sana. (2023). Cybersecurity disclosure in the banking industry: a comparative study. International Journal of Disclosure and Governance, 20(4), 451-477. https://doi.org/10.1057/s41310-023-00190-8

Form 8-K | Investor.gov. (s. d.). U.S Securities and Exchange Comission. Récupéré le 29 juillet 2025 de https://www.investor.gov/introduction-investing/investing-basics/glossary/form-8-k

Form 10-K | Practical Law. (s. d.). Thomson Reuters. Récupéré le 29 juillet 2025 de https://ca.practicallaw.thomsonreuters.com/7-382-3483?transitionType=Default&contextData=(sc.Default)&firstPage=true

Gao, Lei, Calderon, Thomas G. et Tang, Fengchun. (2020). Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems, 38, 100468.

Gerding, Erik. (2023, 14 décembre). SEC.gov | Cybersecurity Disclosure. https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-disclosure-20231214#_ftn1

Hartmann, Caroline C et Carmenate, Jimmy. (2021). Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. Current Issues in Auditing, 15(2), A9-A23. https://doi.org/10.2308/CIIA-2020-034

Harymawan, Iman et Rahmawati, Dwi Ragil. (2022). Effect of Voluntary Risk Management Disclosure and Risk Management Committee on Firm Value. Jurnal Manajemen Teori dan Terapan | Journal of Theory and Applied Management, 15(3), 423-432. https://doi.org/10.20473/jmtt.v15i3.37498

Healy, Paul M et Palepu, Krishna G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. Journal of Accounting and Economics, 31(1-3), 405-440. https://doi.org/10.1016/S0165-4101(01)00018-0

Héroux, Sylvie et Fortin, Anne. (2024). Board of directors' attributes and aspects of cybersecurity disclosure. Journal of Management and Governance, 28(2), 359-404. https://doi.org/10.1007/s10997-022-09660-7

Higgs, Julia L., Pinsker, Robert E., Smith, Thomas J. et Young, George R. (2016). The Relationship between Board-Level Technology Committees and Reported Security Breaches. Journal of Information Systems, 30(3), 79-98. https://doi.org/10.2308/isys-51402

Institut canadien des Comptables agréés. (2006). Circulaire de sollicitation de procurations. Office québécois de la langue française. https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/503061/circulaire-de-sollicitation-de-procurations

Ismail, Aida Maria, Fauzi, Siti Aisyah Amirah Mohd et Yatim, Normahiran. (2022). The Impact of Board Capabilities on Firm Financial Performance: A Resource-Based View Perspective. Archives of Business Research, 10(11), 8-27.

Krause, Ryan, Semadeni, Matthew et Withers, Michael C. (2016). That special someone: When the board views its chair as a resource: That Special Someone. Strategic Management Journal, 37(9), 1990-2002. https://doi.org/10.1002/smj.2444

Kurnia, Pipin et Ardianto, Ardianto. (2024). Board gender diversity and cyber security disclosure in the Indonesian banking industry: a two-tier governance context. Corporate Governance: The International Journal of Business in Society, 24(7), 1614-1637. https://doi.org/10.1108/CG-01-2023-0010

Li, He, No, Won Gyun et Wang, Tawei. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. International Journal of Accounting Information Systems, 30, 40-55. https://doi.org/10.1016/j.accinf.2018.06.003

Lim, Stephen, Matolcsy, Zoltan et Chow, Don. (2007). The association between board composition and different types of voluntary disclosure. European Accounting Review, 16(3), 555-583.

Madhani, Pankaj M. (2017). Diverse Roles of Corporate Board: A Review of Various Corporate Governance Theories. IUP Journal of Corporate Governance, 16(2).

Masoud, Najeb et Al-Utaibi, Ghassan. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. Research in Economics, 76(2), 131-140. https://doi.org/10.1016/j.rie.2022.07.001

Mazumder, Mohammed Mehadi Masud et Hossain, Dewan Mahboob. (2023). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? Journal of Accounting in Emerging Economies, 13(2), 217-239. https://doi.org/10.1108/jaee-07-2021-0237

Office québécois de la langue française. (1982). Analyse de contenu. Office québécois de la langue française. https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8450013/analyse-de-contenu

PwC, Canada. (2023). Rapport annuel Renseignements sur les cybermenaces au Canada, 47.

Radu, Camélia et Smaili, Nadia. (2022). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. Journal of Business Ethics, 177(2), 351-374. https://doi.org/10.1007/s10551-020-04717-9

Sari, Lia, Adam, Mohamad, Fuadah, Luk et Yusnaini. (2024). Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review. KnE Social Sciences. https://doi.org/10.18502/kss.v9i14.16113

SEC. (2011, 13 octobre). CF Disclosure Guidance: Topic No. 2 - Cybersecurity. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm#_edn1

Selective Disclosure and Insider Trading. (2023, 7 avril). U.S Securities and Exchange Comission. https://www.sec.gov/rules-regulations/2000/08/selective-disclosure-insider-trading

Shukla, Manjula et Pandey, Piyush. (2023). Cybersecurity Oversight and Board Diversity: The Disclosure Paradigm. Dans Cyberfeminism and Gender Violence in Social Media (p. 151-173). IGI Global.

Singh, Harmandeep. (2025). Voluntary cybersecurity risk disclosures and firms' characteristics: the moderating role of the knowledge-intensive industry. Asian Journal of Accounting Research. https://doi.org/10.1108/AJAR-12-2023-0413

Smaili, Nadia, Radu, Camélia et Khalili, Amir. (2023). Board effectiveness and cybersecurity disclosure. Journal of Management and Governance, 27(4), 1049-1071. https://doi.org/10.1007/s10997-022-09637-6

Spence, Michael. (1973). l the MIT press. The Quarterly Journal of Economics, 87(3), 355-374.

Statistiques pour la gestion. (2017). McGraw-Hill Education : Chenelière éducation.

Thomas, Jacob K., Zhang, Frank et Zhu, Wei. (2022). Measuring the Information Content of Disclosures: The Role of Return Noise. The Accounting Review, 97(6), 417-443. https://doi.org/10.2308/TAR-2021-0075

Understanding SEC Form 6K: A Guide for Foreign Private Issuers. (2025, 11 avril). FasterCapital. https://fastercapital.com/content/Understanding-SEC-Form-6K--A-Guide-for-Foreign-Private-Issuers.html

Verrecchia, Robert E. (2001). Essays on disclosure. Journal of Accounting and Economics, 32(1-3), 97-180. https://doi.org/10.1016/S0165-4101(01)00025-8

Vo, Hong et Pham, Man Duy. (2025). Beware of false prophets: Cybersecurity risk and strategic voluntary disclosure. The British Accounting Review, 101578. https://doi.org/10.1016/j.bar.2025.101578

Wang, Tawei et Hsu, Carol. (2010). The impact of board structure on information security breaches.

Wang, Tawei, Yen, Ju-Chun et Yoon, Kyunghee. (2022). Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. International Journal of Accounting Information Systems, 46, 100567. https://doi.org/10.1016/j.accinf.2022.100567